DOCUMENT RESUME

ED 046 774	24	SE 010 735

TITLE	Unified Modern Mathematics, Course 2, Part 1.
INSTITUTION	Secondary School Mathematics Curriculum Improvement Study, New York, N.Y.
SPONS AGENCY	Columbia Univ., New York, N.Y. Teachers College.; Office of Education (DHEW), Washington, D.C. Bureau of Research.
BUREAU NO	BR-7-0711
PUB DATE	69
CONTRACT	OEC-1-7-070711-4420
NOTE	337p.
EDRS PRICE	EDRS Price MF-$0.65 HC-$13.16
DESCRIPTORS	Algebra, *Curriculum Development, Geometric Concepts, Geometry, Graphs, *Instructional Materials, Mathematical Logic, *Modern Mathematics, *Secondary School Mathematics, *Textbooks

ABSTRACT

This is Part 1 of the second course in a series which focuses on building fundamental mathematical structures. Topics considered in this book include: an introduction to mathematical logic and mathematical proof, a continuation of the study of groups, an introduction to axiomatic affine geometry, fields, the real number system, and coordinate geometry. The discussion of groups contains an example of a non-commutative group, theorems about groups, and the concept of isomorphism. Axioms for an affine geometry are given together with some logical consequences of these axioms and finite and infinite models for the axioms. The chapters on fields and the real number system include solving equations and inequalities, properties of the real number system and calculation with irrational numbers. (FL)

BR 7-0711
PA 24
SE

ED0 46774

Secondary School Mathematics
Curriculum Improvement Study

UNIFIED MODERN MATHEMATICS

COURSE II

PART I

U.S. DEPARTMENT OF HEALTH, EDUCATION
& WELFARE
OFFICE OF EDUCATION
THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL OFFICE OF EDUCATION POSITION OR POLICY.

TEACHERS COLLEGE COLUMBIA UNIVERSITY

SE 010 735

Secondary School Mathematics
Curriculum Improvement Study

ED046774

UNIFIED MODERN MATHEMATICS

Course II

Part I

Financial support for the Secondary School Mathematics Curriculum Improvement Study has been provided by the United States Office of Education and Teachers College, Columbia University.

UNIFIED MODERN MATHEMATICS, COURSE II was prepared by the Secondary School Mathematics Curriculum Improvement Study with the cooperation of

Nicholas Branca, Teachers College, Columbia University
Gustave Choquet, Universite de Paris, France
Ray Cleveland, University of Calgary, Canada
John Downes, Emory University
Howard F. Fehr, Teachers College, Columbia University
James Fey, Teachers College, Columbia University
Alan Gewirtz, City University of New York
Abraham Glicksman, Bronx High School of Science, New York
Vincent Haag, Franklin and Marshall College
Thomas Hill, University of Oklahoma
Peter Hilton, Cornell University
Julius H. Hlavaty, National Council of Teachers of Mathematics
Michael Hoban CFC, Iona College, New York
Meyer Jordan, City University of New York
Burt Kaufman, Southern Illinois University
Howard Kellogg, Teachers College, Columbia University
Erik Kristensen, Aarhus University, Denmark
Howard Levi, City University of New York
Edgar R. Lorch, Columbia University
Lennart Råde, Chalmers Institute of Technology, Sweden
Myron F. Rosskopf, Teachers College, Columbia University
Harry Ruderman, Hunter College High School, New York
Harry Sitomer, C. W. Post College
Hans-Georg Steiner, University of Karlsruhe, Germany
Marshall H. Stone, University of Massachusetts
Stanley Taback, New York University
H. Laverne Thomas, State University College at Oneonta, N.Y.
Albert W. Tucker, Princeton University
Bruce Vogeli, Teachers College, Columbia University
Lucian Wernick, Teachers College, Columbia University

Copyright, 1969, Teachers College, Columbia University

PERMISSION TO REPRODUCE THIS COPY-
IGHTED MATERIAL HAS BEEN GRANTED
Y
Howard F. Fehr

O ERIC AND ORGANIZATIONS OPERATING
NDER AGREEMENTS WITH THE U.S. OFFICE

CONTENTS

Chapter I: MATHEMATICAL LANGUAGE AND PROOF

1.1 Introduction ....page 1
1.2 Mathematical Statements........................ 2
1.4 Connectives: And, Or.......................... 8
1.6 Conditional and Bi-conditional Statements...... 15
1.8 Quantified Statements.......................... 26
1.9 Substitution Principle for Equality (SPE)...... 32
1.11 Inference..................................... 37
1.13 Direct Mathematical Proof..................... 49
1.14 Indirect Mathematical Proof................... 53
1.16 Summary....................................... 58

Chapter II: GROUPS

2.1 Definition of a Group.......................... 62
2.3 A non-Commutative Group........................ 76
2.5 More on Permutations........................... 89
2.6 Functional Notation............................ 92
2.7 More Notation.................................. 93
2.9 Some theorems About Groups..................... 101
2.11 Isomorphism................................... 109
2.13 Summary....................................... 115

Chapter III: AN INTRODUCTION TO AXIOMATIC AFFINE GEOMETRY

3.1 Preliminary Remarks............................ 119
3.2 Axioms... 120
3.4 Some Logical Consequences of the Axioms........ 128
3.6 A Non-Geometric Model of the Axioms............ 135
3.8 Other Models of the Axioms - Finite and Infinite 142
3.10 Equivalence Classes of Parallel Lines......... 156
3.12 Parallel Projection........................... 162
3.14 Vectors - An Intuitive Introduction........... 174
3.16 Summary....................................... 188

Chapter IV: FIELDS

4.1 What is a Field?............................... 193
4.3 Getting Some Field Theorems Painlessly......... 197
4.4 Trouble with 0................................. 199
4.6 Subtraction and Division in Fields............. 202
4.8 Fractions in Fields............................ 206
4.10 Order in Fields............................... 208

4.12 How Many Ordered Fields?........................ 213
4.13 Equations and Inequations in $(Q,+,\cdot,<)$......... 214
4.15 Solving Quadratic Equations....................... 219
4.17 Summary... 223

Chapter V: THE REAL NUMBER SYSTEM

5.1 The Equation $x^2 = 2$ in $(Q,+,\cdot)$................. 227
5.3 The Measuring Process............................. 230
5.5 The Length of a Line Segment...................... 236
5.7 Three Illustrative Cases.......................... 239
5.9 The Real Number System............................ 244
5.11 Some Properties of the Real Number System...... 249
5.13 Arithmetic of Irrational Numbers............... 257
5.15 Summary.. 260

Chapter VI: COORDINATE GEOMETRY

6.1 Introduction...................................... 265
6.2 Axiom 4. Uniqueness of Line Coordinate Systems 266
6.4 Axiom 5. Relating Two Coordinate Systems on a Line........................ 271
6.6 Segments, Rays, Midpoints......................... 279
6.8 Axiom 6. Parallel Projections and Line Projections...................... 288
6.10 Plane Coordinate Systems........................ 291
6.12 An Equation for a Line.......................... 298
6.14 Intersections of Lines.......................... 303
6.16 Triangles and Quadrilaterals.................... 309
6.18 The Pythagorean Property........................ 314
6.20 Plane Rectangular Coordinate Systems............ 318
6.22 Summary... 325

CHAPTER 1

MATHEMATICAL LANGUAGE AND PROOF

1.1 Introduction

Oh Yeah? Prove It!

How many times have you made a debatable statement and faced a challenge to prove your statement, to convince a doubting listener? When you told some friends you think Willie Mays is a better baseball player than Mickey Mantle? When you told your science teacher that helium is lighter than air? When you told your parents that all the other kids get to stay out late? When you told your mathematics teacher that adding two even numbers always gives an even number?

In each of these situations someone wants to be convinced; he wants proof of your statement. The kind of evidence or argument you present depends on the area of disagreement: Comparison of batting averages drawn from a baseball book of records might settle the Willie Mays-Mickey Mantle argument. A simple experiment with a helium filled balloon might convince the science teacher. And testimony from your best friend might swing your parents to a later Friday night curfew.

Your conjecture about sums of even numbers would be proven according to rules of argument accepted in mathematics. You have already seen and been asked to supply proofs of mathematical statements. In fact, the "even plus even is even" statement was justified as follows:

1. If a and b are even, then $a = 2m$ and $b = 2n$.
2. Then $a + b = 2m + 2n$,
3. $a + b = 2(m + n)$,
4. or $a + b = 2k$, where $k = m + n$.
5. This implies that $a + b$ is even.

What is it that makes this argument an acceptable mathematical proof? What are the rules governing proof in mathematics? Since proof will become an increasingly important part of your work in mathematics, this chapter is designed to explain and illustrate the ground rules of mathematical proof.

1.2 Mathematical Statements

To understand mathematical proof, we must first understand the meaning of the language used in proofs. In ordinary English we frequently allow a word, or a sentence, to have different meanings depending on the context in which it is used. For example, suppose we hear a weather forecast of fair and warm. What does "warm" mean in this sentence? In New York in July "warm" might mean 80°F., while in January we consider 45°F. to be warm. In Miami, Rio, or Casablanca entirely different standards would prevail. The meaning of a simple English sentence often depends in a complex way on the context in which it is used.

Mathematics is a basic tool of science, so mathematical language must be precise. We cannot allow ourselves the freedom of ordinary English usage. For example, the mathematical statement

> A natural number is prime if and only if
> it has exactly two distinct factors

gives clear directions for determining whether a given natural number is or is not prime. 13 has two factors, 13 and 1, and so it is prime. 12 has 6 factors--1, 2, 3, 4, 6, 12--so it is not prime. The mathematical statement defining prime number is precise enough to determine primeness of 12, 13 and any other natural number.

The example just given led to a conclusion that might be written

12 is not prime.

This is an example of a kind of sentence used in mathematics called a statement. Another mathematical statement is

6 is prime.

Of course, this is false, since 6 has four distinct factors: 1, 2, 3, and 6.

> In mathematics, a statement is a sentence
> that is either true or false, but not both.

It may seem strange to be at all interested in false statements. But often we do not know immediately whether a statement is true or false. What about the following statement?

15283 is prime.

One task of the mathematician is to determine the truth or falsity of a given statement, so he must be willing to allow for the possibility that it could be false. However, it must be one or the other: not both and not maybe.

Example 1. "$2 < 5$." This is a statement, and clearly it is true.

Example 2. "$5<2$." This is false--but it is still a statement.

Example 3. "x is a rational number less than $\frac{2}{3}$." For x, try $\frac{1}{3}$: since $\frac{1}{3}$ is rational and less than $\frac{2}{3}$, the sentence is true if x is equal to $\frac{1}{3}$. Now try $\frac{3}{4}$: since $\frac{3}{4}$ is rational and greater than $\frac{2}{3}$, the sentence is false if x equals $\frac{3}{4}$. However, the sentence itself does not tell us the value of x. Therefore, as the sentence is written, it is neither true nor false; it is not a statement. This type of sentence is called an open sentence.

Example 4. "Trenton is the state capital of New Jersey." Although not a mathematical sentence, this sentence is a statement. It is true.

Example 5. "Cross the street!" This sentence is a command, but not a statement, since there is no meaningful way it can be said to be true or false.

Often in this chapter we will want to refer to the same statement several times. To save writing, it is often easier to assign statements letter names such as P, Q, R, etc., and to refer to each statement by writing its letter name rather than the whole statement.

For example, we could write

S: "15,735 is divisible by 5."

Then in future discussions, instead of writing, "15,735 is divisible by 5" we may write simply S. A note of caution: To avoid confusion it must always be clear to which statement a given letter refers, so we must be careful never to use the same letter to refer to more than one statement in the same discussion.

Consider now the statement P: "1271 is prime." At first glance you are probably not able to tell whether P is true or false, though you know that it will be one or the other. If it turns out that P is false, then the statement Q: "1271 is not prime," will be true. But what if P is true after all? Certainly then Q will be false. Thus P and Q are opposites in the sense that if P is true then Q is false and if P is false then Q is true. Given any statement R we can always form a new opposite statement by the same process, and we call this new statement the negation of R. Instead of being assigned a new letter, the negation is called "not R." The relation between a statement and its negation is summarized in Table 1, called a truth table.

R	not R
true	false
false	true

Table 1

Example 6. Suppose S: "$2 + 3 = 4$" (false of course).
Then not S: "$2 + 3 \neq 4$" (true).

Example 7. Suppose T: "4371 is divisible by 9" (false).
Then not T: "4371 is not divisible by 9" (true).

Example 8. If not T: "4371 is not divisible by 9," then
not(not T): "4371 is not not divisible by 9"
or "4371 is divisible by 9," and
not(not T) is the same as T.

1.3 Exercises

In Exercises 1-11 determine whether or not the given sentence is a statement. If it is a statement, tell whether it is true or false. If it is not a statement, give a reason why.

1. 15283 is a prime number.
2. $\frac{7}{13}(\frac{1}{2} + \frac{7}{8} + \frac{2}{5})$ is a rational number greater than $\frac{1}{2}$.
3. Shut the door.
4. x is a whole number less than 9.
5. $\frac{23}{30} + \frac{2}{7} + \frac{1}{6}$ is not greater than 1.
6. 243 is not prime.
7. It is false that 243 is not prime.
8. It is true that it is false that 243 is not prime.
9. 243 is prime.
10. It is false that it is false that 243 is not prime.
11. It is not true that 15283 is prime.

In Exercises 12-18, find the negation of each of the given statements and determine which (the original and its negation) are true and which are false.

12. 721 is prime.

13. $71 \times 27 = 1917$.

14. $\frac{1}{3} + \frac{2}{5} < \frac{3}{5}$.

15. It is false that it is true that 71 is not less than $38 + 35$.

16. T: "1001 is divisible by 13."

17. not T. (See Exercise 16.)

18. not(not T). (See Exercise 16.)

19. If A is "$7 \times 3 = 3$ in Z_9," write a statement expressing

    (a) not A

    (b) not(not A)

    (c) not(not(not A))

20. If R is "29 is not prime," write a statement expressing

    (a) not R

    (b) not(not R)

    (c) not(not(not R))

21. Complete the following: When S is a statement,

    (a) not(not S) is the same as ________________________

    (b) not(not(not S)) is the same as __________________

22. Suppose you had the statement "not(not(not(... Q) ...)" where the word "not" appeared 37 times. What should this be the same as? Can you state a general rule if "not" appeared n times?

1.4 Connectives: And, Or

The compound mathematical sentence

5 is prime and 5 is a multiple of 3,

is composed of two simple statements joined by the connective "and." Is the compound sentence a statement? Is it true or false?

Clearly the statement "5 is prime" is true and "5 is a multiple of 3" is false. It seems reasonable that for the compound sentence to be true both parts must be true. According to this, then the given sentence is false (but is a statement). What probably suggested that both parts had to be true if the whole sentence is considered to be true is the word "and" connecting the two parts. In this case, mathematics agrees with intuition. Statements of the form "P and Q" are true if both P and Q are true and false if either one of them or both, are false.

Example 1. The compound statement "$5<3$ and $2>7$" is false since neither "$5<3$" nor "$2>7$" is true.

Example 2. The compound statement S: "$2 + 3 = 5$ and $4 \neq 7$" is true. Since "$2 + 3 = 5$" is true and "$4 \neq 7$" is true, both parts of S are true and therefore S is true.

Example 3. S: "x is a whole number greater than 5 and x is a whole number less than 8." Of course, this is not a statement--it is an open

> sentence. If x is replaced by 2, the resulting statement is "2 is a whole number less than 8. The second part of this statement is true, but the first part is false, so the compound statement is false. To emphasize: When 2 was substituted for the variable x, the compound open sentence became a false statement. Different substitutions for x might lead to different truth values for the resulting statement.

In ordinary language, another common connection between two parts of a compound sentence is the word "or." This connective is also useful in constructing compound sentences and statements in mathematics. However, when we try to define carefully the use of "or" (as we did for use of "and"), starting from intuition, we run into difficulties. In everyday usage, "or" can mean quite different things. When we say, "It is raining or the sun is shining," we mean that one or the other is happening, but not both. However, when we say, "Maria is always singing or dancing," we do not want to exclude the possibility that she could be doing both.

Since mathematics demands definitions that are independent of context, we must be arbitrary and exclude (in mathematical sentences) one of the possible interpretations for "or." Following the usage agreed upon by mathematicians, we shall say that when P and Q are statements, "P or Q" is a statement that is true whenever P is true or Q is true or both are true.

Example 4. The compound sentence "$2 = 3$ or $4 + 1 = 5$" is a statement. The first part of this statement is false, but the second part is true, so the compound statement is true.

Example 5. Suppose P is "6 is prime" and Q is "Line reflections preserve direction." P is false, and so is Q. Therefore, the compound statement "P or Q" is false.

Example 6. Suppose S is "2/3 is rational" and T is "$-4<3$." Both S and T are true, so by definition, the compound statement "S or T" is also true.

Example 7. "x is a whole number greater than 6 or x is a whole number less than 3" is a compound open sentence. If x is replaced by 2, the first part of S is false, but the second part is true. From the definition, since this is an "or" compound, the statement is true if x is replaced by 2. Similarly if x is replaced by 7, the first part is true and the second part is false, so 7 makes the whole statement true.

> If x is replaced by 4, both parts are false and so the whole sentence is false. To get all the replacements for x that make the sentence a true statement (i.e. the solution set or truth set for x), we need only take all replacements that make the first part true and then all other replacements that make the second part true. This turns out to be the set of whole numbers excluding 3, 4, 5, and 6.

If P and Q are statements, the compound statement "P and Q" is true if both P and Q are true. The compound statement "P or Q" is true if either P or Q or both are true. These conventions are summarized in Table 2. (Recall such a table is called a truth table.)

P	Q	P and Q	P or Q
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Table 2

Close inspection of Table 2 will reveal an interesting and useful relationship between "and," "or," and the process of negation. The statement "P and Q" is false when P is false ("not P" is true) or Q is false ("not Q" is true) or both are false. But this is the same as saying "P and Q" is false when "not P or not Q" is true.

On the other hand, the statement "P or Q" is false when P is false ("not P" is true) and Q is false ("not Q" is true). But this is the same as saying "P or Q" is false when "not P and not Q" is true. Summarizing,

When "not P or not Q" is true then "not (P and Q)"is true.

and

When "not P and not Q" is true then "not (P or Q)" is true.

1.5 Exercises

In exercises 1-10 determine whether the given compound statement is true or false.

1. $3 \neq 7$ or $5 < 4$.
2. $3 \neq 7$ and $5 < 4$.
3. 23 is prime and is divisible by 5.
4. 23 is prime or is divisible by 5.
5. "U or V" where U is "$\frac{11}{12} < \frac{10}{13}$" and V is "$\frac{13}{16} > \frac{15}{18}$."
6. "U and V"
7. "A or B" where A is "Line reflection R does not preserve parallelism" and B is "R preserves direction."
8. "A and B." (See Exercise 7.)
9. "P or Q" where P is "The image of 6 under the dilation $D_{\frac{2}{3}}$ is 4," and Q is "The image of $\frac{1}{2}$ under D_6 is 3."
10. "P and Q." (See Exercise 9.)
11. Suppose that for some statements S and T the compound statement "S or T" is false. What conclusion (if any) can be drawn about the compound statement "S and T"?

What conclusion (if any) can be drawn about "S and T" if "S or T" is true?

12. Suppose that for some statements G and H, the compound statement "G and H" is true. What conclusion (if any) can be drawn about "G or H"? What conclusion (if any) can be drawn about "G or H" if "G and H" is false?

13. Complete the following truth table.

P	Q	not P	not Q	P or Q	(not P) and (not Q)
T	T	F	F	T	F
T	F				
F	T				
F	T				

What relationship do you notice between the last two columns of the table? What can you conclude from this about the relationship between "(not P) and (not Q)" and "P or Q"?

14. Complete the following truth table.

P	Q	not P	not Q	P and Q	(not P) or (not Q)
T	T	F	F	T	F
T	F				
F	T				
F	F				

Compare the last two columns of the table. What does this tell you about the relationship between "(not P) or (not Q)" and "P and Q"?

15. Find the solution sets for the following open sentences:

    P: "x is a whole number greater than 5."

    Q: "x is a whole number less than 9."

    Now find the solution set for the open sentence "P and Q". What relationship do you notice between the solution set for "P and Q" and those for P and Q individually?

16. Suppose you are told that the solution set for open sentence S(x) is set A and that the solution set for open sentence T(x) is set B. What will be the solution set for the open sentence "S(x) and T(x)" in terms of sets A and B?

17. Find the solution sets for the following open sentences.

    V: "y is a whole number between 3 and 7."

    W: "y is a whole number between 5 and 10."

    Find the solution set for the open sentence "V or W." What relationship do you notice between the solution set for "V or W" and those for V and W individually?

18. You are told that the solution set for open sentence M(x) is set C and that the solution set for open sentence N(x) is set D. What will be the solution set for the open sentence "M(x) or N(x)" in terms of set C and set D?

1.6 Conditional and Bi-conditional Statements

Recently, the science editor of a newspaper made the following prediction: "If the United States sends an astronaut to Mars by 1976, then it will send one to Venus by 1980." Right now, of course, no one can say whether this prediction will turn out to be true or false. After 1980, we will know. Under what circumstances will the prediction turn out to be true? turn out to be false?

Suppose, first of all, that the United States does send an astronaut to Mars by 1976 and then goes on to send one to Venus by 1980. The prediction will then have turned out to be true. On the other hand, suppose that while an astronaut is sent to Mars by 1976, none has reached Venus by 1980. In this case, the prediction must be judged false.

These two possibilities are clear enough, but there are two more that require careful thought. Suppose that everything goes wrong, so that not only does an astronaut not make it to Venus in 1980, but none gets to Mars by 1976. Was the science editor wrong? Think carefully. Remember he did not say an astronaut would get to Mars by 1976 or that one would get to Venus by 1980; he only said that if one were sent to Mars by 1976, one would get to Venus by 1980. So in this case, since no astronaut got to Mars by 1976, we cannot say that the science editor's prediction about Venus was false.

Suppose no astronaut gets to Mars by 1976, but one does get to Venus by 1980. Here again, the prediction is certainly not wrong, so we cannot say that it was false.

Consider the following conjecture made about the sum of two whole numbers a and b:

If a and b are odd, then a + b is even.

Imagine that to test this assertion for a large number of cases (that is, different replacements for a and b) you are given an adding machine that will add any two whole numbers and print the result. For each case you must decide whether the assertion was true or false. To make the job easier, the machine automatically selects numbers to be added and prints them before adding. However, it does not always select odd numbers. (Perhaps the same machine is to be used to test other assertions about the sum of two whole numbers.)

The first two numbers the machine selects are 3 and 5. If the assertion is correct at all, since 3 and 5 are indeed odd whole numbers, the result of the addition should be even. And, of course, it is. The machine prints "8." Next, the machine selects 4 and 7 and prints "11" as the sum. We know 11 is not even. Is the assertion wrong in this case? No, all that is wrong is that the machine did not select two odd numbers to start with. The assertion is still good.

When would you decide that the machine had come up with a case for which the "assertion" was false? This would happen only if the machine found two odd numbers with a sum that was not even. Thus, you would have to find two numbers, a and b, such that "a and b are odd numbers" is true, but "a + b is an even number" is false. For *any other* situation the assertion is certainly *not* false.

What do the two examples discussed above have in common? Both are compound sentences of the form

If P, *then* Q.

In each case it seems reasonable to consider the compound sentence a true statement when P is true and Q is true, and it seems reasonable to consider the compound sentence a false statement when P is true and Q is false. In the case that both P and Q are false or in the case that P is false and Q is true, the truth or falsity of the compound sentence is less clear. However, in these cases it would not be reasonable to say the given predictions were false. Therefore, so that every mathematical sentence of the "If P, then Q" form will be classified as true or false, mathematicians have adopted the following convention:

> When P and Q are statements, "If P, then Q" is a statement that is true unless P is true and Q is false.

Statements of the "If P, then Q. form are called *conditional* statements. Statement P is called the *antecedent* and statement Q is called the *consequent*.

If you are puzzled by the agreement to call conditional statements true when the antecedent is false or when both antecedent and consequent are false, it may be of some help to re-read the discussion of the two examples. Then, if you still have doubts, remember that in mathematics it is sometimes necessary to make or accept arbitrary definitions that may not always agree with intuition. (Recall the case of "or" compound statements.) As you gain experience in working with conditional statements, the definition will become more and more acceptable.

Example 1. Suppose S is "$2 + 3 = 5$" and T is "$2 = 5 - 3$." Then the conditional

If S, then T

is true because S and T are both true.

Example 2. "If $3 = -4$ in Z_7, then $-3 = -4$ in Z_7." Here the antecedent "$3 = -4$ in Z_7" is true but the consequent "$-3 = -4$ in Z_7" is false, so the conditional is false.

Example 3. "If $1 + 1 = 3$ in W, then $5 + 4 = 8$ in W." Here both the antecedent and consequent are false. The conditional is true by our definition.

Example 4. "If $4 + 3 = 2$ in Z_5, then $5 + 4 = 1$ in Z_7." Although the two parts of this conditional statement do not seem to be related, "$4 + 3 = 2$ in Z_5" is certainly true, and "$5 + 4 = 1$ in Z_7" is false, so that the conditional statement is false.

Example 5. "If set $S = \{a, b, c\}$ is not a subset of itself, then S has 5 elements." Both antecedent and consequent are false (recall that every set is a subset of itself), so the given conditional is true! The definition must be followed strictly. This points out that just because a conditional is true does not mean that its consequent is automatically true. This follows only if it is also known that the antecedent is true.

As was the case with "and," "or," and "not," the rules for determining truth or falsity of a conditional statement can be summarized in a truth table.

P	Q	If P then Q
T	T	T
T	F	F
F	T	T
F	F	T

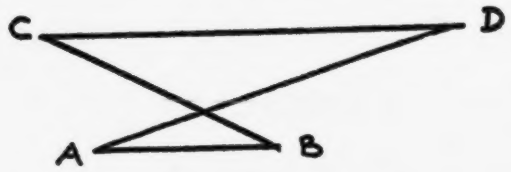
Table 3

Close inspection of this table reveals an important relationship between conditional statements, "and," and the process of negation.

The statement "If P, then Q" is false only when P is true and Q is false (not Q is true). But this is the same as saying "not (If P, then Q)" is true when "P and not Q" is true. Thus, if we can show that the compound sentence "P and not Q" is true, it follows that the conditional "If P, then Q" is false.

Example 6. "If 72 and 27 are multiples of 3, then 72 + 27 is a multiple of 6." Both 72 and 27 are multiples of 3, so the antecedent is true; but $72 + 27 = 99$ is not a multiple of 6, so the consequent is false. Thus, the conditional is false.

Example 7. "If $\overleftrightarrow{AB} \parallel \overleftrightarrow{CD}$, then $\overleftrightarrow{AD} \parallel \overleftrightarrow{BC}$." This is an open conditional sentence. The sketch below shows that the sentence is not true for all points A, B, C, D.



$\overleftrightarrow{AB} \parallel \overleftrightarrow{CD}$, but $\overleftrightarrow{AD} \nparallel \overleftrightarrow{BC}$.

From the conditional it is just a short step to another kind of statement called the bi-conditional. As its name hints (bi is a prefix meaning two), it is in a sense two conditional statements given in one sentence.

Example 8. "A quadrilateral ABCD is a parallelogram if and only if its opposite sides are parallel." This compound statement says "If ABCD is a parallelogram, then its opposite sides are parallel" and "if quadrilateral ABCD has opposite sides parallel, then it is a parallelogram." The original statement of the form "P if and only if Q" stands for two conditionals "If P, then Q" and "If Q, then P."

Example 9. "A mapping is an isometry if and only if it preserves distances between points." This statement may be broken down into the following two conditionals, both of which must be true if the statement is true:

(1) If a mapping is an isometry, then it preserves distances.

(2) If a mapping preserves distances, then it is an isometry.

Examples 8 and 9 illustrate a statement form common in mathematics: If P and Q are statements, "P if and only if Q" is a bi-conditional statement that is true when and only when "If P, then Q" and "If Q, then P" are true.

Suppose for given statements P and Q it is known that "If P, then Q" is true, and suppose furthermore it is known that "If Q, then P" is true. Since "If P, then Q" is true, it is impossible that P is true and Q false. Since "If Q, then P" is true, it is impossible that Q is true and P flase. Since no other possibility is excluded, combining these two conclusions yields either P and Q are both true or both are false. Therefore, the bi-conditional, "P if and only if Q" is a statement that is true whenever P and Q are either both true or both false (otherwise it is false). This is clearly illustrated in Table 4.

P	Q	If P, then Q	If P, then P	P if and only if Q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Table 4

The definition of the bi-conditional is simpler than it appears to be at first. For, suppose that "P if and only if Q" is true. Then if either P or Q is true, the other must automatically be true. Also, if P is false, then Q is false and vice versa. When this happens, that is, when the bi-conditional "P if and only if Q" is true, P and Q are said to be equivalent statements.

The bi-conditional statement, "P if and only if Q," is much stronger than the conditional statement, "If P, then Q." If the conditional statement is true and P is true, then Q will be true. However, if nothing is known about P, but Q is true, we cannot draw any conclusion about P from the conditional. Compare this with the bi-conditional where if Q is true, P must be true.

Example 10. In a plane two lines are parallel if and only if they do not meet." If $\overleftrightarrow{AB} \parallel \overleftrightarrow{CD}$ then $\overleftrightarrow{AB} \cap \overleftrightarrow{CD} = \emptyset$. If $\overleftrightarrow{AB} \cap \overleftrightarrow{CD} = \emptyset$, then $\overleftrightarrow{AB} \parallel \overleftrightarrow{CD}$.

Example 11. "If a and b are even, then $a \cdot b$ is even." 8 and 6 are even and $8 \cdot 6 = 48$ is even. However $6 = 3 \cdot 2$ is even and 3 is not even! (Note: We did not claim $a \cdot b$ is even if and only if a and b are even.)

At the end of Section 1.4 it was pointed out that when a compound statement "not P or not Q" is true, then the statement "not (P and Q)" is true. This was a hint that "not P or not Q" is the negation of "P and Q." In the exercises that followed you proved that this is so by using truth tables (Page 13 , Exercise 14). This can now be stated in a different way: "not (P and Q)" and "not P or not Q" are equivalent statements. The importance of this is that P and Q can be any statements whatsoever, whether true or false. Thus if you wished to show for some statements S and T, that "S and T" is false, (that is, that "not (S and T)" is true), you could show instead that "not S or not T" is true. Similarly, you saw in Exercise 13 on Page 13 , that "not (P or Q)" and "not P and not Q" are equivalent statements, so that if for some statements C and D you wished to show that "C or D" is false, you could show instead that "not C and not D" is true.

Earlier in this section you saw that when the compound sentence "P and not Q" is true, the conditional sentence "if P, then Q" is false (and therefore that "not (if P, then Q)" is true. This suggests that "P and not Q" is the negation of "if P, then Q," or in other words that "P and not Q" and "not (if P, then Q)" are equivalent statements. In the exercises you will be asked to prove this by means of a truth table.

Suppose that two statements are each constructed in some complex way from other statements. For example, suppose that one of these complex statements is "S or (T and U)" and the other is "(S or T) and (S or U)." If it is known that these two complex statements are equivalent, then to show that "S or (T and U)" is true we could show instead that "(S or T) and (S or U)" is true. Again, the importance of this is that (if the two complex statements are in fact equivalent) the equivalence must hold for any statements S, T, and U. (You will be asked to prove this equivalence using a truth table.) The procedure of showing a statement to be true by showing an equivalent statement true is commonly used.

1.7 Exercises

In Exercises 1-13, determine whether the given statement is true or false.

1. If $2 < 5$, then $2 + 3 < 5 + 3$.
2. If 7 is a rational number, then $\frac{5}{7} < \frac{3}{7}$.
3. If a number is odd, then three times the number is odd also.
4. If 6 is odd, then 3×6 is odd also.
5. If wishes were horses, then beggars would ride.
6. "If S, then T" where S is "3 is even and 5 odd" and T is "3 + 5 is even."
7. "If T, then S." (See Exercise 6.)
8. "S if and only if T." (See Exercise 6.)
9. "If Q, then R" where Q is "4 is odd" and R is "3 x 4 is odd."
10. "If R, then Q." (See Exercise 9.)
11. "R if and only if Q." (See Exercise 9.)
12. "Q if and only if R." (See Exercise 9.)
13. If 7 is a prime, then 2 does not divide 7.

14. Write a negation of the conditional statement in Exercise 4.

15. Write a negation of the statements appearing in
   (a) Exercise 6.
   (b) Exercise 7.
   (c) Exercise 8.

16. Write a negation of the statements appearing in
   (a) Exercise 9.
   (b) Exercise 10.
   (c) Exercise 11.

17. Complete the following truth table.

P	Q	not Q	if P, then Q	not(if P, then Q	P and (not Q)
T	T	F	T	F	F
T	F				
F	T				
F	F				

Compare the last two columns. What do you observe? What does this tell you about the relationship between "not(if P, then Q)" and "P and (not Q)"?

18. S = {a, b, c, d}. The following relation R is defined on S:

{(a,a), (b,b), (c,c), (d,d)}.

Note that R is a reflexive relation on S, since xRx is true for every element x in S. Recall that R is symmetric, if when x and y are elements of S and xRy is true, then yRx is true. Is R symmetric? Is R transitive? Explain your answer.

19. Show, by using a truth table, that "S or (T and U)" and "(S or T) and (S or U)" are equivalent.

*20. Show that "if A, then (B or C)" and "if (not C), then (if A, then B)" are equivalent.

1.8 Quantified Statements

Recall an example of the previous section: "If a and b are odd whole numbers, then a + b is an even whole number." You were asked to imagine a machine which would test this assertion for a large number of cases by substituting various numbers for a and b. This assertion is in fact true no matter what whole numbers are chosen to replace a and b. Therefore, the following is true: "For all whole numbers a and b, if a and b are odd, then a + b is even." If someone doubted this assertion, how could he try to prove it false? If he could find one pair of odd whole numbers that had an odd sum, the entire assertion would be false. Even though there might be many pairs which would not contradict it, the given statement claims that for all odd whole numbers a and b, a + b is even. A single contradictory case would defeat the assertion.

The assertion "For all whole numbers x, $x + 5 > 5$" actually falls victim to such a criticism. Certainly 0 is a whole number, but 0 + 5 is not greater than 5. Therefore, the statement "For all whole numbers x, $x + 5 > 5$" is false. Note that 0 is the only whole number which contradicts the assertion. This points out that whenever you make an assertion of the "for all" type you must be certain that you have considered every possible case. Note also that by including the phrase for all, the assertions given become statements (called universal statements) that are true or false. This is in contrast to open sentences like "$3x + 2 = 4$" which are true for some replacements of x and false for others.

Many mathematics theorems are universal statements; for example:

Theorem: For every natural number n, $n(n + 1)$ is an even natural number.

Notice that although the theorem uses the words "for every" instead of "for all," the meaning is the same. Other phrases used having the same meaning are "for each" and "for any," or sometimes simply "each," "any," etc. When these phrases are used to form universal statements, they are called universal quantifiers.

Example 1. "Every natural number is a positive integer." From the definitions of natural number and positive integer, you know that this is true. Note that this statement is not about every number, but about every natural number. Thus the universal quantifier "every" is applied to the set of natural numbers. The set to which the quantifier applies is called the domain of the quantified statement, so the domain of this statement is the set of natural numbers.

Example 2. "Every whole number is a positive integer." This is false, since there is a whole number (0) that is not a positive integer. The universal quantifier used is "every" and the domain of this universal statement is the set of whole numbers.

Example 3. "All line reflections are isometries." As you saw in Course I this is true. It is impossible to find a line reflection that is not an isometry. The domain of this universal statement is the set of line reflections.

Example 4. "Any even number greater than 2 is the sum of two primes."

To show that this is false, you would have to find an even number that cannot be written as the sum of two primes. No one has yet been able to do this (as of 1969); on the other hand, no one has been able to prove this universal statement--known as Goldbach's Conjecture. Note that the domain of this statement is the set of even numbers greater than 2.

Example 5. "For all x and y in Z_6, if $x \cdot y = 0$, then $x = 0$ or $y = 0$."

Fortunately, since Z_6 is a small system, you will be able to test the truth of this conjecture easily.

Now consider the open sentence, "$x + 3 > 7$." By introducing a universal quantifier, the open sentence becomes a statement: "For all whole numbers x, $x + 3 > 7$." This is false, since 3 is a whole number and "$3 + 3 > 7$" is false. The open sentence could be converted into a *true* statement in two different ways. One approach is to change the domain and state "For all whole numbers x greater than 4, $x + 3 > 7$."

Another approach involves a change of quantifiers. Instead of "For all x" we could write "For some x," changing the universal statement to a new form

$$\text{For some } x \text{ in } W,\ x + 3 > 7.$$

Of course, "for some" is not a universal quantifier, and the meaning of the sentence is completely changed. The new sentence will be true if there is one or more whole numbers x for which $x + 3 > 7$. Certainly 5 is one such--so there is no need to look further. The new statement is true.

The phrase "for some" that we used to construct the new statement is called an *existential quantifier,* because it asserts that something exists--in this case, a whole number x for which "$x + 3 > 7$" is true. The statement itself is called an existentially quantified statement, or more simply, an *existential statement*.

Example 6. "For some x in Z_{12}, $x^2 = 4$."

In Z_{12}, $2^2 = 4^2 = 8^2 = 4$.

Therefore the existential statement is true.

Example 7. "For some integer a, a·a is negative."
To show that this is true, you would have to find at least one integer, which when multiplied by itself, would give a negative number. If a is negative, then a·a is positive (recall that the product of two negative numbers is positive) and if a is positive, then a·a is positive also. If $a = 0$, then $a \cdot a = 0$. Therefore there is no integer a such that $a^2 < 0$. Conclusion: The existential statement of this example is false.

Example 8. "There is an isometry that is not a line reflection."
Since there are isometries which are not line reflections (rotations and translations, for example), this existential statement is true. Note that the quantifier is "there is." This has essentially the same meaning as "for some," as you have seen, and is considered to be mathematically the same. Another form of the existential quantifier is "there exists."

Example 9. "There exists an integer x for which $x \cdot x = 9$."
Now $3 \cdot 3 = 9$ and $(-3) \cdot (-3) = 9$, so there are in fact two integers x for which $x \cdot x = 9$; namely

3 and -3. Do not be fooled by the words, "There exists an integer ... " This really means, "There exists at least one integer ... " and therefore the given existential statement is true.

Example 10. "For some odd whole numbers x and y, x + y is is even."

At the beginning of this section, you saw that the universal statement, "For all odd integers x and y, x + y is even," is true. Since "x + y is even" is true for all odd whole numbers x and y, it is certainly true for some of them. The given existential statement is also true.

The negations of the existential and universal statements can be found easily. Suppose that some given statement is, "For all x, P(x)." If this is false, then there must be at least one replacement for x which makes P(x) a false statement. But this is simply saying that "For some x, not P(x)" is true.

Then, "For some x, not P(x)" is the negation of "For all x, P(x)." The negation of "For all whole numbers n, n is prime" is "For some whole number n, n is not prime."

It follows in exactly the same way that the negation of "For some x, Q(x)," is "For all x, not Q(x)." For example, the negation of the statement "For some integer a, a·a is negative," is the statement "For all integers a, a·a is non-negative."

1.9 Substitution Principle for Equality (SPE)

Suppose you are asked to do the following arithmetic problem: $1234 \times 72 + 1234 \times 28$. Naturally, this invdlves a lot of computation unless some shortcut can be found. Perhaps you see one using a property you studied in Course I:

$$\begin{aligned} 1234 \times 72 + 1234 \times 28 &= 1234(72 + 28) \\ &= 1234(100) \\ &= 123,400. \end{aligned}$$

What justifications can be given for these steps? The first is an application of the distributivity of multiplication over addition in the set of integers. In the second step, "100" has been written in place of "72 + 28". What reason could be given for this? Perhaps you would say that this is a known fact of addition of integers. However, more than this is actually involved. For the known fact of addition used here is "72 + 28 = 100." Another way of saying this is that "100" is another name for "72 + 28". Then this name "100" is used in place of the previous name "72 + 28." That is, we have replaced one name for a particualr thing by another name for the same thing. In Course I, the guarantee that this is allowable was called replacement assumption. However, there is a more general principle in mathematics that will permit this kind of replacement and can be applied in a greater variety of situations. This is called the Substitution Principle for Equality (abbreviated SPE) and can be stated as follows:

> If any part of statement is replaced by an expression to which it is equal, the resulting statement is equivalent to the original one. In other words, if the original statement is true, the resulting statement is true; if the original statement is false, then the new one is false also.

In the example given above, 72 + 28 is equal to 100, and since "1234 x 72 + 1234 x 28 = 1234(72 + 28)" is true, then "1234 x 72 + 1234 x 28 = 1234(100)" is true also. In the next step of the example, since 1234(100) = 123,400 and "1234 x 72 + 1234 x 28 = 1234(100)," by SPE, "1234 x 72 + 1234 x 28 = 123,400" is true also.

To see how this principle can be applied to a different kind of problem, consider how you might find the solution set to the open sentence, "3 + a = 5" in Z_7. One way to do this is to add the opposite of 3 to both sides. Since the opposite of 3 in Z_7 is 4,

$$4 + (3 + a) = 4 + 5$$

so $(4 + 3) + a = 2$ (Why?)

so $0 + a = 2$ (Why?)

or $a = 2$ (Why?)

What justifies adding the opposite of 3 to both sides? This is an application of a direct consequence of SPE--the Left Operation Property.

> If (S,o) is an operational system and if x and y are elements of S and x = y, then if z is also in S, $z \circ x = z \circ y$.

In the above example, the operational system is $(Z_7,+)$, and we started with $3 + a = 5$ (so x is $3 + a$ and y is 5). Then z was 4, and "o" was addition, so $z \circ x = z \circ y$ becomes $4 + (3 + a) = 4 + 5$.

To see that left operation is a result of SPE, start with an operational system (S,o) and $x = y$, with both x and y in S. Now if z is in S, then surely $z \circ x = z \circ x$, since equality is reflexive. Since $x = y$, by SPE any x in $z \circ x = z \circ x$ may be replaced by y. Replacing the one on the right by y, the result is $z \circ x = z \circ y$. That is, this is true if $x = y$. But this is just what left operation says.

1.10 Exercises

Determine the truth or falsity of the statements in Exercises 1-15. Then state whether the given statements are universal or existential (or neither) and give the domain.

1. Every line reflection is an isometry.
2. Every isometry is a line reflection.
3. There is a line reflection which is an isometry.
4. There is an isometry which is a line reflection.
5. For all integers x and y, x^2y^2 is even.
6. For some integers x and y, x^2y^2 is even.
7. For each integer x greater than -3 and less than 4, $-2 - x > 0$.
8. There exists an element x in Z_7 for which $x^3 = 3$.
9. There exists an element x in Z_6 for which $x^2 = 2$.

10. For all mappings s and t, $s \circ t = t \circ s$.

11. For some mappings g and h, $g \circ h \neq h \circ g$.

12. For all line reflections ℓ_m, if A is a point in the plane, then $(\ell_m \circ \ell_m)(A) = A$.

13. For every operational system (S,o), if a and b are in S, then $a \circ b = b \circ a$.

14. There is an operational system (T,o) such that for all a,b, and c in T, $a \circ (b \circ c) \neq (a \circ b) \circ c$.

15. For every operational system (U,o), and for all x, y, and z in U, $x \circ (y \circ z) = y \circ (x \circ z)$.

16. Write statements that are negations of the statements in Exercises 1-4. State whether each of your statements is a universal statement, an existential statement, or neither.

17. Write statements that are negations of the statements in Exercises 5 and 6.

18. Write statements that are the negations of the statements in Exercises 10 and 11.

19. Determine the truth or falsity of the following statement and write its negation:

    For each integer s, there exists an integer t such that $t > s$.

20. Determine the truth or falsity of the following statement and write its negation:

    There exists an integer x such that for all integers y, $y > x$.

21. For the following arithmetic problem tell where and how SPE is used:

$$\begin{aligned} 37 \times 53 &= (30 + 7) \times (50 + 3) \\ &= (30 + 7) \times 50 + (30 + 7) \times 3 \\ &= (30 \times 50) + (7 \times 50) + (30 \times 3) + (7 \times 3) \\ &= 1500 + 350 + 90 + 21 \\ &= 1961 \end{aligned}$$

22. A proof is given below of the theorem:

For every integer _r_, $r \cdot 0 = 0$.

Identify the steps in which SPE is used and tell how it is used.

$r \cdot 0 = r \cdot 0$	?
$r \cdot (0 + 0) = r \cdot 0$	?
$r \cdot (0 + 0) = r \cdot 0 + 0$	?
$r \cdot 0 + r \cdot 0 = r \cdot 0 + 0$	?
$r \cdot 0 = 0$	Cancellation Law in (Z,+)

1.11 Inference

Suppose a swimming pool has the following sign posted at the entrance:

If it is a Rainy Day
Then the Pool Will Be Closed

Since we have no reason to believe that the manager of the pool would post false statements, we consider this a true conditional. Now knowing also that it is a rainy day will allow us to draw the conclusion that the pool will be closed. Two statements, both considered true, have given us another true statement.

Look at the above example again, but this time assume we know that the pool is closed. Using only the information given, what conclusions can be drawn about whether it is or is not a rainy day? If you think for a moment, you will realize that the pool could be closed for many reasons other than a rainy day; it might be the middle of winter! Thus, no conclusion can be drawn on the basis of these two true statements.

Let us analyze these two instances closely. Let P represent the statement "it is a rainy day" and Q represent the statement "the pool will be closed." Thus, "if P then Q" represents the statement made by the swimming pool manager, "If it is a rainy day, then the pool will be closed." Knowing only that the compound sentence "if P then Q" is a true statement does not tell us the truth value of the statement P, or the truth value of the statement Q. However, "if P then Q" is a true statement in each of the following 3 cases:

(1) when both P and Q are true,

(2) when P is false and Q is true, and

(3) when both P and Q are false.

Thus, one of the 3 cases must hold when "if P then Q" is true. If in addition to knowing "if P then Q" is true, we also know P is true (as in the first situation) then the only case which could hold is (1), since it is the only case of the three in which P is true. Thus according to Case (1), both P and Q must be true and we have obtained additional information; namely that Q is a true statement. To repeat, knowing that both statements, P and "if P then Q" are true, we can conclude that the statement Q is also true. We express this, the first of our inference rules, as:

(1) From "If P, then Q" and "P," we infer "Q."

In mathematics, reasoning from a true conditional statement "if P then Q" and a true antecedent P to the truth of the consequent Q is following a basic rule of inference called the rule of detachment or modus ponens.

If we again consider the three cases in which "If P, then Q" is true, we can see why it is impossible to draw a conclusion from knowledge that Q is true. When "if P then Q" is true and Q is true, two possibilities exist for P -- P true or P false -- and we cannot draw a conclusion from the information given. To repeat, having as true the conditional "if P then Q" and the consequent Q, does not give any information about the truth value of P.

Example 1. For each of the following accept the following conditional statement as true:

If it is Saturday, then the school is closed.

a) Accepting also as true in addition to the conditional, the statement "It is Saturday" leads us to infer the conclusion "The school is closed." This is a direct application of the rule of detachment.

b) Accepting as true the statement "The school is closed" along with the conditional does not allow us to make any inferences about what day of the week it is. This is an example of the form "If P then Q" and "Q."

Example 2. In each of the following accept the first two statements as true.

a) If 7 has exactly two distinct factors, then 7 is a prime number. 7 has exactly two distinct factors.

Conclusion:

7 is a prime number.

b) If a natural number has exactly two distinct factors,

Then it is a prime number.

7 has exactly two distinct factors.

Conclusion:

7 is a prime number.

Discussion: In each of the above examples the rule of detachment has been used. However, example (b) does not fit the form exactly. Another rule of inference has been used. The conditional statement "If a natural number has exactly two distinct factors, then it is a prime number," can be considered as a perfectly legitimate true statement. However it cannot be expressed as a compound of simpler statements since the simple sentences contained within, "A natural number has exactly two distinct factors," and "It is a prime number," are not statements. That is they are not either true or false but open sentences.

Conditionals of this form are called general or universal statements. Accepting them as true means we interpret them to be true for all substitution instances. We are saying "If a natural number $\underline{x}$ has exactly two distinct factors, then $\underline{x}$ is a prime number," is a true statement for any and every substitution for the variable $\underline{x}$ from the domain of natural numbers.

Thus in example (b), from the universal conditional alone we can infer the conditional "If 7 has exactly two distinct factors then 7 is a prime number." Making this inference first we can then proceed as in example (a) to use the rule of detachment and conclude "7 is a prime number."

This inference rule called inference from a universal statement is often used in mathematics since many statements are universal conditionals. Often the particular statement inferred from the universal is not mentioned as was done in example (b). In most cases the argument will be clear enough without adding extra steps. However, it is important to realize when you are making inferences from universal statements.

Example 3. For each of the following accept the following conditional statement as true:

If a number is divisible by 8, then it is divisible by 4.

(a) If, in addition to the above conditional, the statement "256 is divisible by 8" is accepted as true, then the conclusion "256 is divisible by 4" must be accepted as true.

(b) However, if the statement "68 is divisible by 4" is accepted as true, no conclusion about divisibility of 68 can be inferred.

(c) In the same way, if "736 is divisible by 4" is accepted as true, then no conclusion about divisibility of 736 by 8 can be inferred.

(d) If the statement "25 is divisible by 8" is accepted as true, then the conclusion "25 is divisible by 4" must be accepted as true.

Discussion: Both Examples 3(a) and 3(d) are of the following form: "If P, then Q" is accepted as true and P is accepted as true. This implies that Q must be accepted as true. In

Example 3(d), 25 is in fact not divisible by 8 nor is it divisible by 4. However, accepting 25 as divisible by 8 must, by the rule of detachment, lead to accepting it as divisible by 4. The use of inference is correct and the statements are consistent.

Examples 3(b) and 3(c) are of the form: "If P, then Q" is accepted as true and Q is accepted as true. On the basis of this information alone we cannot make any inferences about the truth or falsity of P. In Example 3(c), although 736 is divisible by 8, this additional information is not a logical consequence of the two statements accepted as true.

Example 4. For each of the following, accept as true the conditional statement: "If a and b are both even integers, then a + b is an even integer."

(a) Accepting as true "6 and 10 are both even integers" leads to the conclusion "6 + 10 is an even integer."

(b) Accepting as true "13 + 3 is an even integer" does not imply that 13 and 3 are even, a good thing, since they are clearly both odd.

(c) Accepting as true "12 + 4 is an even integer" does not itself imply that 12 and 4 are even -- although they are, in fact, both even.

Let us again consider the swimming pool example. However, this time, in addition to assuming that, "If it is a rainy day, then the pool will be closed," is a true statement, assume that we know the pool is not closed. We can then conclude that it is not a rainy day! We may write this, the second of our inference rules, as:

(2) From "If P, then Q" and "not Q" we infer "not P."

Looking again at the three cases in which "If P, then Q" is true, we can see that in only

1. P true and Q true
2. P false and Q true
3. P false and Q false

one (Case 3) is Q false. In that case P also is false, so "If P, then Q" is true and "not Q" is true must imply "not P" is true. Again, knowledge about the truth of two statements have allowed us to draw a conclusion about a third statement. If, instead of knowing the pool is not closed, we know it is not a rainy day, then we are again in a situation where no conclusion can be drawn. The pool could be open or closed. This is the form "if P then Q" true and P false, and can be either Case (2) where Q is true or Case (3) where Q is false.

Example 5. Assume "If a whole number is divisible by 8, then it is divisible by 4."

(a) Accepting as true "82 is not divisible by 4" leads to the conclusion "82 is not divisible by 8."

(b) Accepting as true "876 is not divisible by 8" leads to no conclusion about divisibility about 4.

(c) Accepting as true "534 is not divisible by 4" leads to the conclusion "534 is not divisible by 8".

Example 6. "For all integers $p > 2$, if p is prime, then p is odd."

(a) 257 is a prime greater than 2, so 257 is odd.

(b) 684 is greater than 2 and not odd, so 684 is not prime.

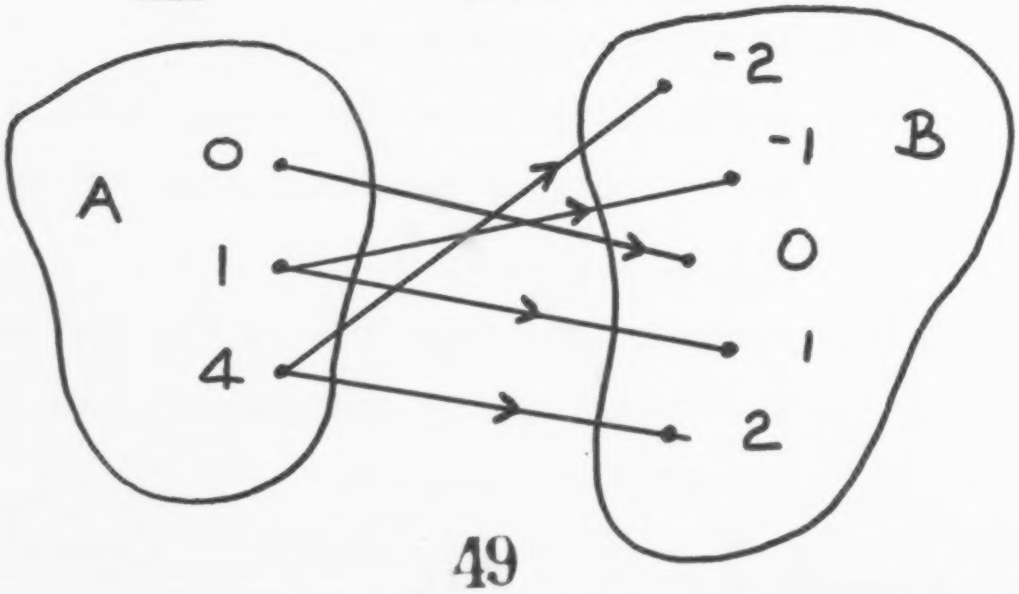
Example 7. "All isometries preserve angle measure."

(a) Line reflections are isometries, so they preserve angle measure.

(b) Mappings that don't preserve angle measure are not isometries.

(c) Dilations preserve angle measure, but they are not isometries!

Example 8. A mapping assigns only one image to each domain element. In the diagram below, 4 has two assigned images, so the diagram does not define a mapping from A to B.



The Law of Detachment is the most common and important type of logical inference in mathematics. There are, however, several other basic reasoning patterns used in mathematical argument.

Suppose we accept the following compound statement as true:

25 is an odd number and 25 is a perfect square.

From this one statement alone, we may certainly conclude that 25 is a perfect square. (We may also conclude that 25 is an odd number.) Here, accepting as true a compound statement, where the connective used is and, allows us to accept as true each of the simple statements involved. The reverse is also useful. That is, accepting as true two statements allows us to infer that the compound and statement formed by them is also true.

Suppose we accept as true the compound statement:

529 is a perfect square or 529 is divisible by 13.

From this statement alone, no inferences can be made. However, if we also accept as true the statement "529 is not divisible by 13," then we must accept as true the statement "529 is a perfect square."

The three inference rules described above may be expressed as follows:

(3) From "P and Q" we infer "P."

(4) From "P" and "Q" we infer "P and Q."

(5) From "P or Q" and "not Q" we infer "P."

The five rules of inference are valuable tools in the analysis of reasoning problems.

Example 9. Assume the following three statements are true:

(a) If we have an art class, then it is Friday.

(b) We have a music class or we have an art class.

(c) It is not Friday.

Conclusion: We have a music class.

Discussion: From the conditional statement (a) and the negation of its consequent, (c), we infer, by inference rule (2), that we do not have an art class. Using this fact and (b), we infer, by inference rule(5), that we have a music class. If P is "We have an art class" and Q "It is Friday" and R "We have a music class" the argument takes the following form"

(a)	If P then Q	ASSUMED TRUE
(b)	R or P	ASSUMED TRUE
(c)	Not Q	ASSUMED TRUE
(d)	Not P	From (a) and (c); rule (2).
(e)	R	From (b) and (d); rule (5).

1.12 Exercises

In Exercises 1-14 assume the given statements are true.

(1) State the inferences (if any) that can be made.

(2) Assign letter names to each of the component simple statements and state the inference rules used in drawing your conclusions.

1. If I toss a fair coin, then the probability of getting a tail is $\frac{1}{2}$.
   I toss a fair coin.
2. If set A is a subset of every set, then set A is the empty set.
   Set A is not the empty set.
3. If sets A and B are the complements of each other, then the union of the two sets is the universe.
   The union of set A and set B is the universe.
4. If the image of point A under a reflection in point P is A', then P is the midpoint of $\overline{AA'}$.
   The image of point A under a reflection in point P is A'.
5. m is parallel to n or m is parallel to p.
   m is parallel to n.
6. If B is between A and C, then $AB + BC = AC$.
   $AB + BC \neq AC$.
7. The natural number 7 is even or it is odd.
   7 is not even.
8. If *x* and *y* are both positive, then their product is positive.
   The product of *x* and *y* is positive.
9. If the sum of *a* and *b* is negative, then at least one of *a*,*b* is negative.
   The sum of *a* and *b* is positive.
10. If *x* and *y* are both positive, then their product is positive.
    x and *y* are not both positive.

*11. If *a* and *b* are rational numbers, then there is a rational number between them.
   a and *b* are rational numbers greater than 5.

*12. If $x \geq 8$, then $y \geq 5$.
$|x - 5| > 3$ and $y < 5$.

13. If a number is divisible by 8, then it is divisible by 4.
If a number is divisible by 4, then it is divisible by 2.
88 is divisible by 8.

14. $x = 3$ or $x = 4$. If $x = 3$, then $y = 7$.
$y \neq 7$.

15. If $\overrightarrow{AC} = \overrightarrow{AB}$, then B is on $\overrightarrow{AC}$.
$\overrightarrow{AC} = \overrightarrow{AB}$ or $\overrightarrow{AC} \cap \overrightarrow{AB} = A$.
B not on $\overrightarrow{AC}$.

16. A mathematics teacher, moonlighting as a detective, was investigating a crime. He had come to accept the following statements as true:

(1) The butler or the stepson murdered Mr. X.

(2) If the butler murdered Mr. X, then the murder did not occur before midnight.

(3) If the stepson's testimony is correct, then the murder occurred before midnight.

(4) If the stepson's testimony is incorrect, then the house lights were not turned off at midnight.

(5) The house lights were turned off at midnight, and the butler is not wealthy.

Using his knowledge of logic and proof, the mathematico-detective quickly inferred who the murderer was. Who was the murderer and what rules of inference did the sleuth use to discover this?

1.13 Direct Mathematical Proof

Section 1.1 of this chapter sketched an argument justifying the statement:

If *a* and *b* are even whole numbers,
then $a + b$ is even.

What made that argument acceptable as a mathematical proof? Let's examine that argument.

The statement to be proven is a conditional of the form "If P, then Q where P is "*a* and *b* are even whole numbers" and Q is "$a + b$ is even." The conditional will be true unless P is true and Q is false. Therefore the strategy of argument is to assume P true and show that then Q must also be true.

Proof:

1. *a* and *b* are even whole numbers.	1. Assume P true.
2. $a = 2x$ for some *x* in W. $b = 2y$ for some *y* in W.	2. Definition: A whole number *n* is even if and only if $n = 2m$ for some *m* in W.
3. $a + b = 2x + b$.	3. Right operation on $a = 2x$ by *b* in $(W,+)$.
4. $a + b = 2x + 2y$.	4. SPE in Step 3 since $b = 2y$.
5. $2x + 2y = 2(x + y)$.	5. Distributive property of $(W,+,\cdot)$.

6. $a + b = 2(x + y)$.	6. SPE using Step 5 in Step 4.
7. $x + y$ is in W.	7. (W,+) is an operational system.
8. $a + b$ is even	8. Definition in Step 2.

Analysis: The proof is a sequence of statements leading to the desired conclusion "a + b is even." Each step of the argument is justified by some known fact, axiom, definition, or theorem about whole numbers, *or* by an acceptable inference from earlier statements in the proof.

Step 1. a and b are even whole numbers. The strategy of proof is to assume the truth of this statement and show that "a + b is even" must then be true also.

Step 2. From "a and b are even whole numbers," we infer "a is an even whole number" by rule (3) of inference. Similarly we infer "b is an even whole number." The definition of even whole number states that n is even if and only if $n = 2m$ for some m in W. In particular, since a is even, $a = 2x$ for some x in W; and since b is even, $b = 2y$ for some y in W.

Step 3. The right operation principle states that for any x, y, z in S, if $x = y$, then $x \circ z = y \circ z$ in the operational system (S,o). In particular, if $z = b$, then $a + b = 2x + b$ in (W,+).

Step 4. Since step 2 states that $b = 2y$, S P E and step 3 justify inferring the statement: $a + b = 2x + 2y$.

Step 5. The distributive property of $(W,+,\cdot)$ states that if p, q, r are in W, then $p(q + r) = pq + pr$. Since 2, x, and y are in W, the rule of detachment justifies the statement: $2x + 2y = 2(x + y)$.

Step 6. Using the statements of steps 5 and 4, S P E justifies inferring: $a + b = 2(x + y)$.

Step 7. If x and y are in W, then $(x + y)$ is in W because $(W,+)$ is an operational system. In step 2, x and y were guaranteed to be in W; thus the law of detachment justifies the assertion: $(x + y)$ in W.

Step 8. The definition of even number given in step 2 also states that if $n = 2m$ for some m in W, then n is even. In particular, $a + b = 2(x + y)$ and $x + y$ is in W, so the law of detachment justifies the inference: $a + b$ is even.

The point of the above discussion is to indicate the many inference rules used in constructing a mathematical proof. Axioms and theorems are usually conditional statements; definitions are usually biconditional statements. Thus, in using an axiom, theorem, or definition to justify a step in a proof, we are in reality using the rule of detachment and possibly other rules of inference depending on whether we have compound or simple statements.

It is important to realize that all steps in a proof must be justifiable. However, only rarely is every reason stated. Rather, an abbreviated form is usually offered. The degree of abbreviation used in a proof depends to a great extent on the individuals to whom the proof is directed. Thus, in advanced mathematics books, we are likely to find the words, "It is obvious that ... follows," where quite a few statements and inference rules are called for.

The next sample proof gives another mathematical argument. Examine it to see how rules of inference, axioms, theorems, and definitions are used in the steps leading to the desired conclusion. This proof has another feature--an argument by cases--that is worth close attention.

Theorem. Let a and b be whole numbers. If a or b is an even number, then a·b is even.

Proof. The conditional is true unless the antecedent is true and the consequent is false. Therefore, the strategy is to assume "a or b even" is true and show that "a·b even" must follow.

1. a or b even	1. Assumption

2. Assume *a* is even	2. One of *a* or *b* must be even, so we give an argument for the case *a* is even. A similar argument works for the case *b* is even.
3. $a = 2x$ for some x in W.	3. Definition of even whole number.
4. $a \cdot b = (2x)b$	4. Right operation.
5. $(2x)b = 2(xb)$	5. Associativity of multiplication in $(W,\cdot)$.
6. $a \cdot b = 2(xb)$	6. S P E step 5 in step 4.
7. xb is in W.	7. $(W,\cdot)$ is an operational system (x is in W by step 3 and b is in W by assumption).
8. $a \cdot b$ is even	8. Definition of even number and results of step 6 and 7.

1.14 Indirect Mathematical Proof.

The preceding examples of proofs illustrated a direct approach to proof of a conditional statement like "If P, then Q." The strategy was to assume P true and show that Q must then also be true. There is a more devious approach, suitably called *indirect proof*, which is often very useful.

The conditional "If P, then Q" is true unless P is true and Q is false. To show the conditional true, one must show that any time the consequent Q is false, the antecedent P must also be false. Assume "not Q" and show "not P" follows. (Recall that this is rule (2) of inference.) This is the strategy used in the following proof.

Theorem. Let *a* and *b* be whole numbers. If a·b is odd, then *a* is odd and *b* is odd.

Proof. In this conditional, P is "a·b is odd" and Q is "*a* odd and *b* odd." The strategy is to assume Q false and show that then P must be false also.

1. not (*a* odd and *b* odd).	1. Assumption.
2. *a* even or *b* even	2. An *and* compound statement is false if one of its component statements is false.
3. a·b is even	3. The preceding theorem stated that if *a* or *b* is even, then a·b is even.
4. a·b is not odd	4. By definition every whole number is even if and only if it is not odd.

Check the role of inference patterns, such as detachment, in this proof.

The next theorem is proven by another form of the indirect method. It rests again, however, on the fact that a conditional

"If P, then Q" is true unless P is true and Q is false. In this proof we assume that the worst has happened--P is true and Q is false--and show that such a situation is impossible because it leads to a contradiction of an axiom, theorem, or definition.

Theorem. If n is a whole number, then $n(n + 1)$ is even.

Proof.

1. n is a whole number and $n(n + 1)$ is odd.	1. Assumption
2. n odd and $(n + 1)$ odd	2. By the preceding theorem, if ab is odd, then a is odd and b is odd.
3. $n + (n + 1)$ is even	3. By a theorem discussed in Section 1.6, the sum of two odd integers is even.
4. $n + (n + 1) = 2n + 1$	4. Properties of $(W,+,\cdot)$.
5. $2n + 1$ is odd	5. Equivalent to definition of odd number.
6. $n + (n + 1)$ is odd	6. S P E step 4 in step 5.
7. $n + (n + 1)$ is both even and odd.	7. Steps 3 and 6.

Step 7 cannot be true since every even whole number is not odd and every odd whole number is not even. Therefore, the assumption "P and (not Q)" has led to a false statement and must itself be false.

In your future study of mathematics you will often be asked to prove conditional statements of the form "If P, then Q." The most successful strategy depends on the nature of the given statement. It will be helpful to keep in mind these facts:

1. "If P, then Q" is true unless P is true and Q is false.
2. To show "P and (not Q)" impossible, one might try the following:
    (a) Assume P true and show that Q follows.
    (b) Assume "not Q" and show that "not P" follows.
    (c) Assume "P and (not Q)" and show this leads to contradiction of an axiom, theorem, or definition.

1.15 Exercises

In this chapter we have discussed the following five theorems about whole numbers:

Theorem A. If a and b are even, then a + b is even (1.13).

Theorem B. If a and b are odd, then a + b is even (1.6).

Theorem C. If a or b is even, the a·b is even (1.13).

Theorem D. If a·b is odd, then a is odd and b is odd (1.14).

Theorem E. If n is a whole number, then n(n + 1) is even (1.14).

1. Give a step by step analysis of the following proof of Theorem C, taken from the text. Use the analysis of Theorem A as a guide and give both justifications and explanations of the inference rules used.

1. a or b is even.
2. Assume a is even.
3. a = 2x for some x in W.
4. a·b = (2x)b.
5. (2x)b = 2(xb).
6. a·b = 2(xb).
7. xb is in W.
8. a·b is even.

2. Follow the directions of Exercise 1 in giving analysis of the following proof.

Theorem. Let a, b, and c be whole numbers. If a divides b and b divides c, then a divides c.

Proof. A direct strategy is used.

1. a divides b and b divides c.
2. a divides b.
3. b = ax for some x in W.
4. b divides c.
5. c = by for some y in W.
6. c = (ax)y.
7. (ax)y = a(xy).
8. c = a(xy).
9. xy is in W.
10. a divides c.

In Exercises 3-5 use only theorems A - E and known facts of arithmetic to prove the given assertions.

3. If a + b is odd and a is even, then b is odd.
4. If a + b is even, then a is even and b is even.
5. If a, b, and c are odd, then ab + ac is even.

1.16 Summary

The purpose of this chapter is to illustrate and explain the most common forms of statement and reasoning used in mathematics. The content of mathematical statements may range from facts about number systems to geometry, sets, relations, mappings, or probability. Yet, in each of these areas the statements and methods of reasoning have similar forms and obey common rules of usage.

1. A statement is a sentence that is either true or false, but not both.
2. If P and Q are statements, then "not P," "P and Q," "If P, then Q," and "P if and only if Q" are also statements. The truth or falsity of these compound statements can be determined from the truth or falsity of P and Q according to rules summarized in the following table:

P	Q	not P	P and Q	P or Q	If P, then Q	P iff Q*
T	T	F	T	T	T	T
T	F	—	F	T	F	F
F	T	T	F	T	T	F
F	F	—	F	F	T	T

*("iff" is a common abbreviation for "if and only if.")

3. If P(x) is an open sentence, the universal statement "For all x, P(x)" is true if each replacement of x (from the appropriate domain) makes P(x) a true statement. The existential statement "For some x, P(x)" is true if at least one replacement of x (from

the appropriate domain) makes P(x) a true statement.

4. The rules of inference used are as follows:
   (1) From "If P, then Q" and "P" we infer "Q."
   (2) From "If P, then Q" and "not Q" we infer "not P."
   (3) From "P and Q" we infer "P."
   (4) From "P" and "Q" we infer "P and Q."
   (5) From "P or Q" and "not Q" we infer "P."
5. The substitution principle of equality (SPE) is a basic inference rule.
6. Conditional statements "If P, then Q" are true except when P is true and Q is false. Three strategies of proof are used to establish truth of such conditionals.
   (a) Assume P true and show, by a sequence of inferences, that Q must then be true also.
   (b) Assume Q false and show that P must in that case be false also.
   (c) Assume P true and Q false and show that such a situation leads to the contradiction of an axiom, definition, or theorem.

1.17 Review Exercises

1. For each of the following sentences, determine whether or not the sentence is a statement. If a sentence is a statement, determine whether it is true or false. If a sentence is not a statement, explain why it is not.
   (a) $3 + 5 = 8$.

(b) New York is larger than Chicago.

(c) Go to the store.

(d) $(W, \div)$ is an operational system.

(e) 5 is a perfect square.

2. For each of the following pairs of sentences write each of "P or Q," "P and Q," "not P," "not(P or Q)," "not(P and Q)," "not P," in idiomatic English.

   (a) P: 5 and 6 are consecutive integers.

   Q: The sum of two negative integers is negative.

   (b) P: In tossing a fair coin, $P(\text{Heads}) = \frac{1}{2}$.

   Q: Every prime number has exactly two factors.

   (c) P: $9 + 8 > 19$.

   Q: Some triangles have four sides.

   (d) P: Paris is a beautiful city.

   Q: All cats have nine lives.

3. For each of the following pairs of statements, form "If P, then Q" and determine the truth of the resulting conditional. (Assume that a, b, c, and x are whole numbers.)

   (a) P: $a > b$.

   Q: $a + c > b + c$.

   (b) P: $x \neq 0$.

   Q: $x^2 > 0$.

   *(c) P: $\frac{x}{x} \neq 1$.

   Q: $x = 0$.

4. Use your knowledge of the conditional statement to draw whatever inference is valid in the following situations. If no inference can be made, explain why.

(a) If the water is cold, then I do not go swimming.
The water is cold.

(b) If the water is cold, then I do not go swimming.
I am swimming.

(c) If the water is cold, then I do not go swimming.
The water is not cold.

(d) If angle A and angle B are right angles, then they have equal measure.
Angle A and angle B have equal measure.

(e) If the Yankees play well, then they will win the pennant.
Either the Yankees or the Tigers will win the pennant.
The Yankees and the Tigers will not both win the pennant.
The Tigers won the pennant.

(f) If x is an integer, then x^2 is an integer.
742 is an integer.

CHAPTER 2

GROUPS

2.1 Definition of a Group

Evariste Galois (1811-1832) is generally given credit for first using the group concept and beginning a systematic study of groups. At the age of 19, using group ideas, he resolved a problem regarding solving equations that had challenged the best mathematicians of his time. He was killed in a duel before the age of twenty-one. You may want to read a history of this brilliant mathematician who made an outstanding contribution to mathematics before he reached the age of 20. (Almost any book on the history of mathematics talks about E. Galois; also, most large encyclopedias.)

We shall soon see that a group is a special kind of mathematical system having certain properties. In fact you have already met a number of groups in earlier chapters, one being (Z,+). What makes a mathematical system a group? Why take time to study groups? This chapter will answer these two questions. Let us try to answer the second question first, namely, why take time to study groups.

We often invest time and money with the hope that the investment will, in the long run, save both time and money. Witness the tremendous investments made in constructing bridges, tunnels, skyscrapers, supersonic planes, atom smashers, etc. Not only have these investments saved time and money but they have also reduced discomfort and increased our enjoyment of life. A study of groups will serve a similar function. It will help us save time by enabling us to solve many problems all at once instead of having to work each problem separately. A study of groups will also give us a deeper insight into the nature of mathematics and enable us to view a great many apparently isolated operational systems as a single entity.

A very simple example of solving a large class of problems simultaneously follows. Suppose you had a great many equations to solve, like the following:

$$\begin{array}{ll} 2x + 3 = 19 & 473x + 297 = 16\frac{1}{3} \\ 7x - 11 = 28 & 8.76x - 4.93 = 7.89 \end{array}$$

You could solve each one separately, or you could recognize that all of these equations take the form

$$ax + b = c \qquad \text{where } a, b, c, \text{ are rational numbers, } a \neq 0.$$

Solving the last equation for x in terms of a, b, c will give us a formula for solving all such equations. You can imitate the solution for the first equation to obtain a solution for the last one as follows:

$$\begin{array}{ll} 2x + 3 = 19 & ax + b = c \\ 2x \quad = 19 - 3 & ax \quad = c - b \\ x \quad = \frac{19 - 3}{2} & x \quad = \frac{c - b}{a} \\ \text{Solution Set} = \{8\} & \text{Solution Set} = \{\frac{c - b}{a}\} \end{array}$$

Hence whenever we know the values of a, b, c with $a \neq 0$, a solution may be obtained by using these values in the formula

$\frac{c - b}{a}$. For example, for the equation $7x - 11 = 28$ we have $a = 7$, $b = -11$, $c = 28$. Hence $\frac{c - b}{a} = \frac{28 - (-11)}{7} = \frac{39}{7} = 5\frac{4}{7}$, and our solution set is $\{5\frac{4}{7}\}$. Formulas like this are useful in programming a computer to solve our problems.

Let us now give a very simple example of two different equations whose solutions have a striking similarity of another kind.

$3x = 12$	$3 + x = 12$
$\frac{1}{3}(3x) = \frac{1}{3}(12)$	$(-3) + (3 + x) = (-3) + 12$
$(\frac{1}{3}\cdot 3)x = 4$	$((-3) + 3) + x = 9$
$1\cdot x = 4$	$0 + x = 9$
$x = 4$	$x = 9$
Solution Set = $\{4\}$	Solution Set = $\{9\}$

Note the parallel steps in both solutions. A study of groups will show how both equations are essentially of the same type.

We now look at some mathematical systems that are groups and some that are not. Perhaps you will recognize the properties that are common to the groups.

It will be convenient to adopt the following abbreviations. If S is any set of numbers let

S^{+} = {Positive numbers of S}
S^{-} = {Negative numbers of S}
$S^{\pm}$ = {Non-zero numbers of S}.

The left column below will have examples of operational systems that are groups, while the right column will have operational systems that are not groups.

These are groups:

Ex. 1 $(Z,+)$

Ex. 2 $(Q^{+},\cdot)$

Ex. 3 $(Q^{\pm},\cdot)$

Ex. 4 $(Z_4,+)$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ex. 5 $(\{e,x,y,z\},o)$:

o	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

These are not groups:

Ex. 1' $(Z,-)$

Ex. 2' $(Q^{+},+)$

Ex. 3' $(Q^{\pm},+)$

Ex. 4' $(Z_4\setminus\{0\},\cdot)$:

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Ex. 5' $(\{e,x,y,z\},o)$:

o	e	x	y	z
e	e	x	y	z
x	e	x	y	z
y	e	x	y	z
z	e	x	y	z

You may want to try to discover for yourself why the systems on the left are groups while those on the right are not. What do the groups have in common?

1. First of all a group must be an operational system. Recall that this requires that it be a set together with a binary operation defined on the set. Thus, to every pair of elements (a,b) in the set, there is assigned a unique element of the set. If we agree to use "o" for the operation of the group whose elements compose set S, then whenever $a \in S$ and $b \in S$, it follows

that $a \circ b \in S$. This statement includes the possibility that $a = b$. Note that in $(Z,+)$, Z is the set of integers while $+$ (addition) is the group operation on Z. Hence, whenever a and b are integers $a + b$ is a unique integer.

2. The group operation is associative. Thus whenever a, b, c are in S we have $(a \circ b) \circ c = a \circ (b \circ c)$. For $(Z,+)$ this condition becomes the familiar property that whenever a, b, c are integers,

$$(a + b) + c = a + (b + c).$$

For $(Q^+,\cdot)$, the associative property becomes

$$(a\cdot b)\cdot c = a\cdot(b\cdot c)$$

whenever a, b, c are positive rational numbers.

3. Among the elements of S, there is an element which we shall denote by e such that

$$a \circ e = e \circ a = a \text{ for every element } a \in S.$$

For $(Z,+)$, $e = 0$ and $a + 0 = 0 + a = a$ for every integer a. For $(Q^+,\cdot)$, $e = 1$ and $a\cdot 1 = 1\cdot a = a$ for every positive rational number a. We call e the identity or the identity element, and refer to possession of the identity element as having the identity property.

4. There is only one more requirement for a group $(S,\circ)$. With every element $a \in S$ there is associated a unique element in S, which we shall denote by a^I, having the property

$$a \circ a^I = a^I \circ a = e$$

where e is the identity element in S. We call a^I the inverse of a, and refer to possession of an inverse element (for each element) as having the inverse property. For (Z,+) we have $a^I = -a$ and $a + (-a) = (-a) + a = 0$ for every integer a. For $(Q^+,\cdot)$ we have $a^I = \frac{1}{a}$ and $a\cdot\frac{1}{a} = \frac{1}{a}\cdot a = 1$, for every positive rational number a.

We summarize by giving a definition of a group. Recall that an operational system (S,o) consists of a set S, and a binary operation o defined on the elements of S such that for every pair of elements a, b in S, aob is a uniquely determined element of S.

Definition. A group is an operational system (S,o) with the following three properties:

1. Associative Property. For all a, b, c in S

   $$(aob)oc = ao(boc).$$

2. Identity Property. There is exactly one element in S, denoted by e, such that for every element a in S,

   $$aoe = eoa = a$$

   e is called the identity element of the group.

3. Inverse Property. To each element a in S, there corresponds exactly one element in S, denoted by a^I, such that

   $$aoa^I = a^Ioa = e.$$

   a^I is called the inverse of a.

Note: The e in Property 3 is of course the identity element described in Property 2.

Another example of a group is $(Z_8,+)$. (You should be able to show that this system possesses all of the properties of a group. Perhaps you can convince yourself that associativity holds by trying a few cases; consideration of every possible case here is too time consuming.) Now the set Z_8 contains the following elements:

0, 1, 2, 3, 4, 5, 6, 7.

Suppose we take the following subset of Z_8:

$$T = \{0,2,4,6\},$$

and keep the original group operation. We can then construct the following table:

+	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

"+" here is Z_8 addition.

Every ordered pair of elements in T has an assignment in T. Therefore, (T,+) is an operational system in its own right. Furthermore, it is a group. Showing that (T,+) possesses the group properties is easy:

1) (T,+) is of course associative since it "comes from" the group $(Z_8,+)$.
2) The identity element 0 is an element of T.
3) 0 is its own inverse; 4 is its own inverse; 2 and 6 are inverses of each other.

Since T is a subset of the original set Z_8, we say that the group (T,+) is a subgroup of the group (Z_8,+). And we make the following definition of a subgroup:

Definition. (T,o) is a subgroup of (S,o) if and only if both (T,o) and (S,o) are groups, and $T \subset S$.

Example 6. (Z,+) is the group of integers under addition. Let E denote the set of even integers, a subset of Z. Is (E,+) a subgroup of (Z,+)?

First, (E,+) is an operational system, since every pair of elements of E is assigned an element of E. (The sum of two even integers is an even integer.)

Second, (E,+) has the associate property, since (Z,+) has.

Third, the identity element 0 is in the set E of even integers.

Fourth, every element of E has an inverse in E. For instance, the inverse of the even integer 2 is the even integer -2.

Therefore, (E,+) is a group; it is a subgroup of (Z,+).

Example 7. ($Z_5 \backslash \{0\}, \cdot$) is a group; the table is shown below.

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Let T = {1,2}. Is (T,·), where · is the original group operation, a subgroup of $(Z_5\backslash\{0\},\cdot)$? Examination of the table below shows that we do

·	1	2
1	1	2
2	2	4

not even have an operational system; the pair (2,2) is assigned 4, which is not an element of T. Therefore, (T,·) is not a subgroup of $(Z_5\backslash\{0\},\cdot)$.

In the exercises, you will have an opportunity to identify other subgroups. Also you may want to try to prove the following theorem (see Exercise 13) which is often useful in making a decision as to whether or not a system is a subgroup of a given group.

Theorem. If (S,o) is a group, and $T \subset S$, then (T,o) is a subgroup of (S,o) if (T,o) is an operational system, and every element of T has its inverse in T.

2.2 Exercises

1. Find the identity element for each of the following:
   (a) $(Q^{\pm},\cdot)$
   (b) Ex. 4 of text: $(Z_4,+)$
   (c) Ex. 5 of text: ({e,x,y,z},o)
2. Find the inverse
   (a) for 5 in (Z,+).

(b) for 5 in $(Q^+,\cdot)$.

(c) for 3 in Ex. 4 of text: $(Z_4,+)$.

(d) for x in Ex. 5 of text: $(\{e,x,y,z\},o)$.

(e) for 5 in $(Z_7\setminus\{0\},\cdot)$.

3. Why is each of the following not a group?

(a) $(Z,-)$

(b) $(Q^-,\cdot)$

(c) $(Q,\cdot)$

(d) $(Q^{\pm},+)$

(e) Ex. 4' of text

(f) Ex. 5' of text

(g) $(Z^+,+)$

(h) $(Z^{\pm},+)$

(i) $(Z,\cdot)$

(j) $(Q^+,+)$

(k) $(Z^-,+)$

(l) $(Z_8\setminus\{0\},-)$

(m) $(Q^-,+)$

(n) $(Z_4,\cdot)$

4. Complete the following table for the operation "followed by" denoted by "o" where:

S is the command "Stand Still."

L is the command "Left Face."

A is the command "About Face."

R is the command "Right Face."

o	S	L	A	R
S				
L			R	
A				
R				

The entry in the table shows that "Left Face" followed by "About Face" is equivalent to "Right Face" or that L o A = R.

(a) What is the set of elements here?

(b) What is the binary operation?

(c) What is the identity element?

(d) Does each element have an inverse?

(e) Is it true that:

  (1) $(L \circ A) \circ R = L \circ (A \circ R)$

  (2) $L^I = R$

  (3) $A^I = A$

  (4) $(A \circ R)^I = R^I \circ A^I$

(f) Do you think that we have a group here? The possession of which property is most difficult to deduce? Why?

5. Construct an addition table for $\{(0,0), (0,1), (1,0), (1,1)\}$ where addition is defined by

$(a,b) + (c,d) = (a+c, b+d)$ and the table

+	0	1
0	0	1
1	1	0

Thus, $(1,1) + (1,0) = (0,1)$.

(a) What is the identity element?

(b) What is the inverse of $(0,1)$?

(c) Check associativity of a triple.

(d) Do you think that we have a group here?

6. Consider (Q,av) where av is the average operation defined by

$$(a,b) \xrightarrow{av} \frac{a+b}{2}.$$

(a) Is av a binary operation on the set of rational numbers?

(b) Is (Q,av) a group? Why?

7. $(Z_5\backslash\{0\},\cdot)$ is a group, and $T = \{1,4\}\subset Z_5\backslash\{0\}$. Decide whether or not $(T,\cdot)$ is a subgroup of $(Z_5\backslash\{0\},\cdot)$ by answering the following questions:

(a) Is $(T,\cdot)$ an operational system?

(b) Is the operation $\cdot$ associative in $(T,\cdot)$?

(c) Does $(T,\cdot)$ have an identity element?

(d) What is the inverse of 1? of 4?

(Compare your results here with Example 7 in the text.)

*8. Try to find an operational system

having these properties	but	not these:
(a) Associative, Identity		Inverse
(b) Identity, Inverse		Associative
(c) Associative		Identity, Inverse
(d) Identity		Associative, Inverse

9. (a) Is $(\{1,3,5,7,\},+)$ a subgroup of $(Z_8,+)$?

(b) Is $(\{0,4\},+)$ a subgroup of $(Z_8,+)$?

(c) Construct an operational table for $(Z_7\backslash\{0\},\cdot)$. Is this operational system a group? If so, can you find a subgroup?

10. Let D be the set of odd integers. Is (D,+) a subgroup of (Z,+)? (Compare your answer here with Example 6 in the text.)

11. Decide whether or not each of the following is a subgroup of (Z,+):

(a) (Multiples of 3,+)

(b) (Multiples of 5,+)

(c) ({1,4,7,10,13},+)

12. If we let 5Z denote the multiples of 5, 3Z the multiples of 3, etc., do you think that (nZ,+) is a subgroup of (Z,+) for any n ∈ W?

*13. Prove the theorem in the text. That is, show that (T,o) is a subgroup of the group (S,o) provided that:

(T,o) is an operational system, and

if x ∈ T, then the inverse of x is in T.

(Hints. How do you know that (T,o) must possess the associative property? How do you know that the identity element of the group (S,o) must be in the set T?)

14. Consider all the subsets of {a,b}. If A and B are two subsets, define AΔB to be the set of elements that are either in A or in B but not in both. For example, {a,b}Δ{a} = {b}.

(a) Construct a table for the operation Δ with all subsets of {a,b} for elements.

(b) What is the identity element in the table?

(c) What is the inverse of {b}?

(d) Check associativity.

(e) Do you think that this is a group? Why?

15. Do Exercise 14 for the subsets of {a,b,c}.

16. Consider the following set:

$\{(x, y): x \in \{0,1\}, y \in \{0,1,2\}\}$, and define addition of ordered pairs by

$$(x_1, y_1) + (x_2, y_2) = (x_1 +_2 x_2, y_1 +_3 y_2)$$

where the addition $+_3$ of elements is Z_3 clock addition and $+_2$ is Z_2 clock addition.

(a) List all possible ordered pairs.

(b) Construct an addition table for this operation. What is the identity element?

17. Show that each of the following is a group, and find its identity element.

(a) $(Z,+)$

(b) $(Q\setminus\{0\},\cdot)$

18. Define 2^n in the usual way ($2^1 = 2$, $2^2 = 4$, $2^3 = 8$, etc.) when n is a positive integer. Define $2^0 = 1$. For negative exponents, define $2^{-1} = \frac{1}{2^1} = \frac{1}{2}$, $2^{-2} = \frac{1}{2^2} = \frac{1}{4}$, $2^{-3} = \frac{1}{2^3} = \frac{1}{8}$, etc. We now have 2^n defined for all positive, zero and negative integers n.

We now define the operation by $2^a \cdot 2^b = 2^{a+b}$, for example, $2^3 \cdot 2^5 = 2^8$, $2^{-7} \cdot 2^5 = 2^{-2}$, $2^0 \cdot 2^{-8} = 2^{-8}$

$2^7 \cdot 2^{-7} = 2^0 = 1$.

(a) Show that the system $(\{2^n : n \in Z\},\cdot)$ is an operational system

(b) Show that it is a group.

(c) Find the identity element

(d) Find the inverse of 2^4, 2^{-3}, 2^1, 2^0.

19. Prove that $(Z_n,\cdot)$ is never a group, for any positive integer $n > 1$.

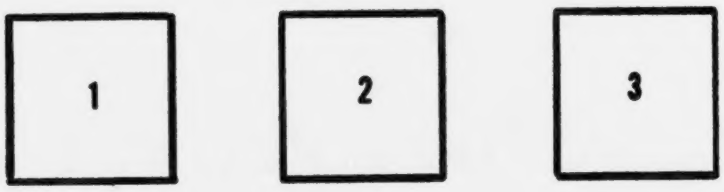
*20. Prove that $(Z_n\setminus\{o\},\cdot)$ is not a group for any even positive integer n.

*21. Prove that $(Z_n\setminus\{o\},\cdot)$ is not a group if n can be written $n = p\cdot q$, where p and q are both positive integers greater

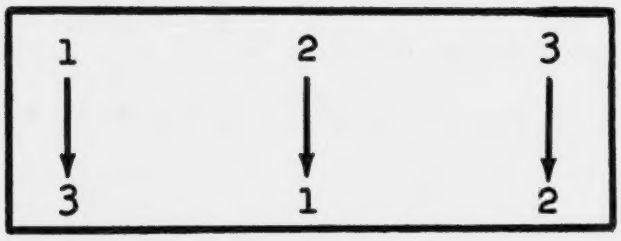
2.3 A Non-Commutative Group

Each of the groups (S,o) so far considered has had an operation that was commutative. By this we mean that for every pair of elements a and b in S, a o b = b o a. Our definition of a group does not insist upon this condition. In fact, there are important groups with operations that are not commutative.

A gym floor has these marks on it.



Pictured are 3 spots for 3 students to occupy. Instructions are given to the students occupying these spots by flashing a card. The following card, for example



is an instruction for:

the student at spot 1 to move to spot 3.

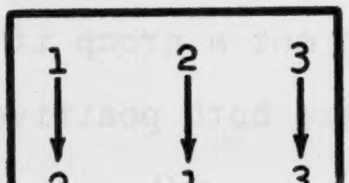
the student at spot 2 to move to spot 1.

the student at spot 3 to move to spot 2.

Let us simplify this instruction card by writing

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Similarly, the instruction



which we simplify to

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

is the instruction for:

the student at spot 1 to move to spot 2.

the student at spot 2 to move to spot 1.

the student at spot 3 to stay at spot 3.

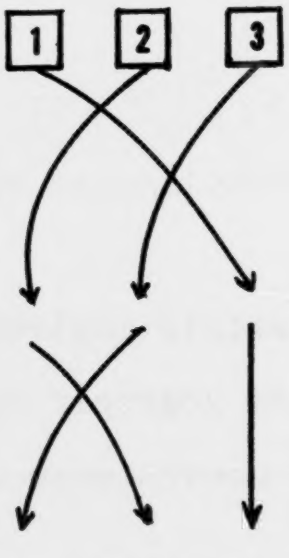
We would like to know what single instruction would result in the same final position as the instruction

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ followed by } \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

We may use the following diagram to help us visualize what is happening.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



The effect of the two instructions, first $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, then $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ can be read from this diagram as $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

We may also view the effects of the instructions by the following diagram:

$$\begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix} \qquad \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}$$

$$\begin{array}{ccccc}1 & \longrightarrow & 3 & \longrightarrow & 3\\2 & \longrightarrow & 1 & \longrightarrow & 2\\3 & \longrightarrow & 2 & \longrightarrow & 1\end{array}$$

Comparing the first and last columns we obtain the combined instruction

$$\begin{array}{ccc}1 & \longrightarrow & 3\\2 & \longrightarrow & 2\\3 & \longrightarrow & 1\end{array} \qquad \text{or} \qquad \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}$$

In other words, using "o" to mean "followed by," we may summarize as follows:

$$\begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}$$

Note that the first instruction is written to the left of the operation sign.

There are but 6 possible instruction cards for 3 spots. You may want to find them yourself before reading on. We list them below and for convenience use the abbreviations: e, p, q, r, s, t.

$$e = \begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix} \qquad r = \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}$$

$$p = \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix} \qquad s = \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}$$

$q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\qquad$ $t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

With these abbreviations we may now construct an operation table. First note that our illustrative exercise

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

corresponds to

$$q \circ t = s.$$

Let us compute $r \circ s$, or

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

which may be visualized by :

$$1 \longrightarrow 1 \longrightarrow 3 \quad \text{so that} \quad 1 \longrightarrow 3$$
$$2 \longrightarrow 3 \longrightarrow 1 \quad \text{so that} \quad 2 \longrightarrow 1$$
$$3 \longrightarrow 2 \longrightarrow 2 \quad \text{so that} \quad 3 \longrightarrow 2$$

Hence $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

or $\qquad r \circ s = q.$

Proceeding in this manner we may compute the operation table:

o	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	q	e	s	t	r
q	q	e	p	t	r	s
r	r	t	s	e	q	p
s	s	r	t	p	e	q
t	t	s	r	q	p	e

The table informs us that o is a binary operation on the set $\{e,p,q,r,s,t\}$, and that $(\{e,p,q,r,s,t\},o)$ is an operational system. This binary operation does not have the usual commutative property that most of our previous operations had. In fact

$$t \text{ o } s = p,$$

while

$$s \text{ o } t = q.$$

Hence

$$t \text{ o } s \neq s \text{ o } t.$$

This one counterexample suffices for the operation o to be classified as a non-commutative operation.

The instructions e,p,q,r,s,t are often called permutations because each one permutes or rearranges the locations of the students. Thus, we may think of the permutation p as an instruction that shifts the students a, b, c initially ordered as abc to the new order bca. We say that bca is an arrangement of abc. We shall also say that abc is an arrangement of abc. Note that each permutation is a 1-1 mapping whose range is the same as its domain. For our example, each permutation produces an arrangement of abc having a different order. Corresponding to the six permutations we have six arrangements of abc:

e: abc

p: bca

q: cab

r: acb

s: cba

t: bac

In general a permutation defined on a set S is a 1-1 mapping having S for both its domain and range. A permutation is thus a one-to-one onto mapping

A permutation may have an infinite domain. For example on Q the following mappings are permutations:

$$n \longrightarrow n + 2$$

$$n \longrightarrow 3n$$

$$n \longrightarrow 3n + 2$$

$$n \longrightarrow an + b, \ a \neq 0.$$

Each is a 1-1 mapping with Q for its domain and range. We shall say more about permutations a little later.

Let us extend our notation for permutations on a set of three elements to a set of four. We could have begun with four spots on a gym floor. The instruction

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

would then correspond to the instruction for the student:

at spot 1 to move to spot 3
at spot 2 to move to spot 4
at spot 3 to move to spot 2
at spot 4 to move to spot 1,

which we may also view as:

$$1 \longrightarrow 3$$

$$2 \longrightarrow 4$$

$$3 \longrightarrow 2$$

$$4 \longrightarrow 1$$

If this instruction is followed by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

we obtain as the combined instruction

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

because:

$1 \longrightarrow 3 \longrightarrow 4$ so that $1 \longrightarrow 4$

$2 \longrightarrow 4 \longrightarrow 1$ so that $2 \longrightarrow 1$

$3 \longrightarrow 2 \longrightarrow 3$ so that $3 \longrightarrow 3$

$4 \longrightarrow 1 \longrightarrow 2$ so that $4 \longrightarrow 2$

If the four students a, b, c, d, had initially the arrangement abcd, then the first permutation would result in the arrangement cdba. As you can guess, there are just as many arrangements of a, b, c, d as there are permutations defined on {a,b,c,d}. Can you guess how many there actually are?

One way of finding out is by writing them all out. Before doing this, let us see if we can obtain this number by a reasoning process. It gets quite tedious to write out all the arrangements when we have 5 or more elements.

For each arrangement of abc we have 4 arrangements of abcd where a, b, c have the same relative order. For the arrangement abc we may insert d into any of 4 places shown by the 4 arrows:

$$\updownarrow \; a \; \downarrow \; b \; \downarrow \; c \; \downarrow$$

to give the 4 arrangements of abcd:

d a b c
a d b c
a b d c
a b c d

What we did for abc holds true for each of the 6 arrangements abc can have, yielding:

d a b c   d b c a   d c a b
a d b c   b d c a   c d a b
a b d c   b c d a   c a d b
a b c d   b c a d   c a b d

d a c b   d c b a   d b a c
a d c b   c d b a   b d a c
a c d b   c b d a   b a d c
a c b d   c b a d   b a c d

The total is 4 x 6 or 24 possible arrangements. Now that we know how many arrangements (or permutations) there are for four elements, how do we figure out the number for 5 elements? The same kind of reasoning tells us that the fifth element may be inserted into any one of 5 places, so that there ought to be (and there are) 24 x 5 or 120 arrangements (or permutations) for 5 elements. If we organize our information on this point you may see a pattern.

Number of Elements	Number of Arrangements
1	1
2	$1\cdot 2$ or 2
3	$1\cdot 2\cdot 3$ or 6
4	$1\cdot 2\cdot 3\cdot 4$ or 24
5	$1\cdot 2\cdot 3\cdot 4\cdot 5$ or 120

We denote $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ by "5!" and read it "five factorial." If n is a positive whole number we have a symbol to denote the product $1 \cdot 2 \cdot 3 \cdot 4 \cdots n$; namely "n!" read "n factorial" or "factorial n." Thus

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n$$

In particular $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = (5!) \cdot 6 = 120 \cdot 6 = 720$

The above pattern suggests that the number of permutations on a set of n elements is n!, which is also the number of arrangements of n things on a line.

We now would like to show that the system $(\{e,p,q,r,s,t\},o)$ consisting of the set of permutations on 3 elements, with the operation "followed by " (denoted by "o") is a group. The table shows that for any permutations x and y in the set $\{e,p,q,r,s,t\}$, xoy is also a permutation in that set, which means that we have an operational system. We must still show three things.

1. Does the system $(\{e,p,q,r,s,t\},o)$ have the identity property? Examining the table we see that there is exactly one identity element, namely,

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

   We conclude that our system has the identity property.

2. Does the system $(\{e,p,q,r,s,t,\},o)$ have the inverse property? From the table, it is easy to see

$$e^I = e \qquad r^I = r$$
$$p^I = q \qquad s^I = s$$
$$q^I = p \qquad t^I = t$$

   Hence the system has the inverse property.

3. Does the system $(\{e,p,q,r,s,t,\},o)$ have the associative

property? To test this completely requires a great many tests. (How many?) We try just one. From the table we see:

$$(p \circ r) \circ t = s \circ t = q$$

$$p \circ (r \circ t) = p \circ p = q$$

Thus $(p \circ r) \circ t = p \circ (r \circ t)$. If we test all triples of elements, we will find that the system does indeed have the associative property.

All the conditions for $(\{e,p,q,r,s,t\},\circ)$ to be a group are satisfied, and so $(\{e,p,q,r,s,t\},\circ)$ is a group, and, in fact, a non-commutative group. Since its elements are permutations on 3 objects we refer to this group as the group of permutations on 3 objects.

2.4 Exercises

1. This exercise will be based on the permutation group on 3 elements: $(\{e,p,q,r,s,t\},\circ)$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad r = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

o	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	q	e	s	t	r
q	q	e	p	t	r	s
r	r	t	s	e	q	p
s	s	r	t	p	e	q
t	t	s	r	q	p	e

(a) We can think of the 6 elements of the permutation group as acting on objects occupying spots 1, 2, 3. For example, the effect of t on the arrangement abc is to change it to bac. List the effect of each element of the permutation group on abc.

(b) Which permutations do not alter the original position of the first element? the second? the third?

(c) Find the solution set for each of the following equations.

(1) $p \circ x = r$

(2) $x \circ p = r$

(3) $x \circ q = t$

(4) $q \circ x = t$

(5) $x \circ x = e$

(6) $x \circ x = p$

(7) $x \circ x = r$

(8) $x^I = p \circ r$

(9) $x^I = r \circ s$

(10) $x^I \circ p = r$

(11) $p \circ x = x \circ p$

(12) $r \circ x = x \circ r$

(13) $(p \circ x) \circ q = r$

(14) $(q \circ x) \circ p = r$

(15) $(x \circ p) \circ x = p$

(16) $(x \circ r) \circ x = r$

(17) $x \circ p = q \circ x$

(18) $(x \circ p)^I = r$

(19) $(x \circ p)^I = x \circ q$

(20) $(x \circ p \circ x)^I = x \circ q$

(d) Compute:

(1) $(p \circ q)^I$, $p^I \circ q^I$, $q^I \circ p^I$ Which are equal?

(2) $(p \circ r)^I$, $p^I \circ r^I$, $r^I \circ p^I$ Which are equal?

(3) $(q \circ t)^I$, $q^I \circ t^I$ $t^I \circ q^I$ Which are equal?

Conjecture a generalization from your answers to (1), (2), and (3).

(4) $(p^I)^I$, $(q^I)^I$, $(r^I)^I$ and conjecture a generalization.

(e) Prove that $(\{e,p,q\},\circ)$ is a subgroup of $(\{e,p,q,r,s,t\},\circ)$.

*(f) Find all the subgroups of ({e,p,q,r,s,t},o).

(g) One of the subgroups of ({e,p,q,r,s,t},o) is ({e,r},o). We may partition {e,p,q,r,s,t} using {e,r} as follows:

- (i) Select an element of {e,p,q,r,s,t} not in {e,r}, say p.
- (ii) Form a new set by operating on each element of {e,r} with p on the left getting {p o e, p o r} or {p,s} .
- (iii) Select an element not in {e,r} or {p,s}, say t.
- (iv) Form a new set by operating on each element of {e,r} with t on the left, getting {t o e, t o r} or {t,q}.

We have partitioned {e,p,q,r,s,t} into sets {e,r}, {p,r}, {t,q} . No two of these sets has an element in common.

- (1) Carry out a partitioning of {e,p,q,r,s,t} by using {e,r} and elements other than p and t.
- (2) Carry out a partitioning by operating on the right, instead of on the left.
- (3) Try to carry out a partitioning by starting with the subset:
  - (a) {e,s}
  - (b) {e,t}
  - (c) {e,p,q}

2. Compute the following:

(a) $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \text{and}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

(b) $$\left[\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\right] \circ$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \text{and} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ$$

$$\left[\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}\right]$$

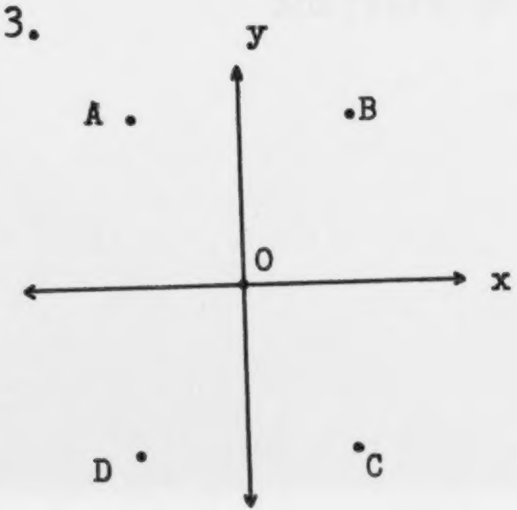
(c) $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{I} \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}^{I}$$

(d) $$\left[\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\right]^{I} \text{and}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}^{I} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{I}$$

Are they equal?

3.



Let x and y be perpendicular lines in a plane, and A,B,C,D the points indicated. Consider the following:

e the identity mapping

ℓ_x the reflection in line x

ℓ_y the reflection in line y

P_o the half turn with center o

These mappings effect permutations on points A,B,C,D. For example the effect of e on A,B,C,D may be written:

$$e = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$$

(a) Complete the expression for ℓ_x or a permutation of ABCD:

$$\ell x = \begin{pmatrix} A & B & C & D \\ D & C & & \end{pmatrix}$$

(b) Write ℓy as a permutation of ABCD.

(c) Do the same for Po.

(d) Complete the operation table, where "o" means "followed by."

o	e	ℓ_x	ℓ_y	P_o
e				
ℓ_x				
ℓ_y				
P_o				

(e) Check whether $(\{e,\ell_x,\ell y,P_o\},o)$ is a group.

2.5 More on Permutations

Let S be the finite set {a,b,c,d,e}. Let f be a one-to-one mapping of S into S. In particular, suppose f is the mapping illustrated in Figure 2.1.

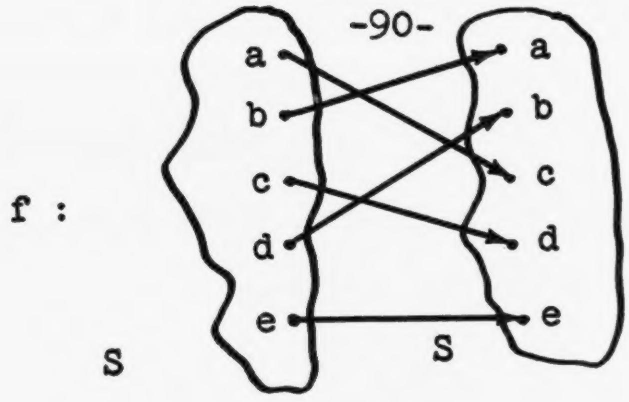


Figure 2.1

We cannot help noticing that f is also the permutation $\begin{pmatrix} a & b & c & d & e \\ c & a & d & b & e \end{pmatrix}$. If we try other one-to-one mappings of S into S, each would yield a corresponding permutation. This suggests that if S is any finite set, and f any one-to-one mapping of S into S, then S is a permutation; that is, a one-to-one mapping in which S is both the domain and range. To prove that a one-to-one mapping of S into S is a permutation, it is sufficient to show that it is an onto mapping. (Do you see why?) This can be proved as follows:

Let S be a finite set having n elements x_1, x_2, ..., x_n. We may write

$$S = \{x_1, x_2, \ldots, x_n\}$$

Let f be any 1-1 mapping of S into S. f maps each element x_i of S into some element, call it x'_i, of S. We diagram the mapping on Figure 2.2.

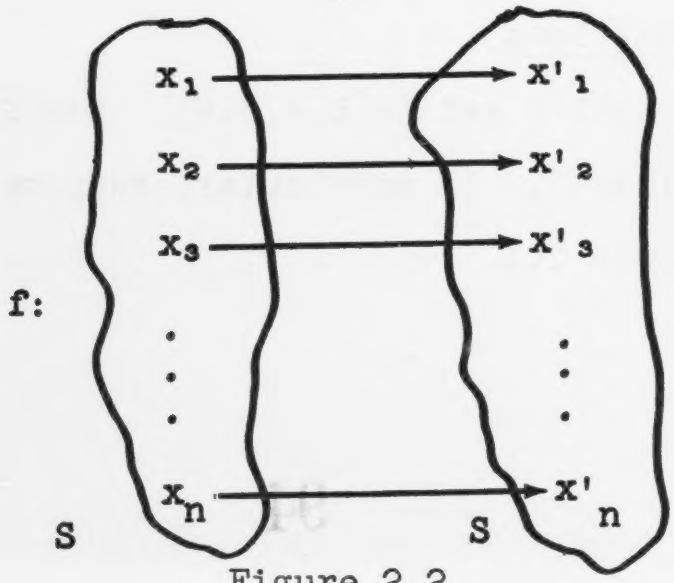


Figure 2.2

Note that x_1, x_2, ... , x_n are the elements of S, and x'_1, x'_2, ... , x'_n are also elements of S.

To show that the mapping f is onto, we must show that each element of S is the image of some element of S, under f. Take any element x_r of S. Suppose it is not the image, under f, of any element of S. Then f maps the n points of S onto (at most) n-1 points of S, since it doesn't map any point on x_r. Thus f maps at least 2 of the points of S onto 1 point. This contradicts the fact that S is a one-to-one mapping. Our supposition must therefore be false, and we conclude that f is an onto mapping. Since f is given as a one-to-one mapping, it is therefore a permutation.

We have thus proved that if S is a finite set, and f a one-to-one mapping of S into S, then f is an onto mapping.

It is not hard to prove a similar result; that is, if S is a finite set and f is an onto mapping from S to S, then f is a one-to-one mapping. In this case, if S contains n elements, then the range of f, being S, contains n elements. If the mapping were not one-to-one, there would be at least two elements in the domain S of f which map into the same element. Since each element of S is the image of at least one element of S (by the definition of onto), it follows that the domain of the mapping would have to contain more than n elements. This is impossible, since the domain is S. We conclude that if S is a finite set, and f is an onto mapping from S to S, then f is one-to-one.

Combining the two results we have that if S is a finite set, and f a mapping from S to S, then f is a one-to-one if, and only if, it is onto. (This means that if f is one-to-one, then it is onto; and if f is onto, then it is one-to-one.)

We will abbreviate one-to-one as "1-1."

The situation for infinite sets is, as you might suspect, different. It is possible for a mapping f to be 1-1 and not onto or onto and not 1-1. Consider the following examples.

Example of a mapping which is 1-1 but not onto:

Let $S = \{1,2,3,\ldots\}$.

$f\colon\ n \longrightarrow 2n$ is a mapping from S into S.

Example of a mapping which is onto but not 1-1:

Let $S = \{1,2,3,\ldots\}$

$$f\colon \begin{array}{ll} n \longrightarrow \frac{n}{2} & \text{if } n \text{ is even} \\ n \longrightarrow \frac{n+1}{2} & \text{if } n \text{ is odd} \end{array}$$

is a mapping from S into S.

We may picture this mapping as

$$f\colon \begin{tikzcd} 1 \arrow[dr] & & 2 \arrow[dl] & 3 \arrow[dr] & & 4 \arrow[dl] & 5 \arrow[dr] & & 6 \arrow[dl] & \cdots \\ & 1 & & & 2 & & & 3 & & \cdots \end{tikzcd}$$

2.6 Functional Notation

The elements of the system $(\{e,p,q,r,s,t\},o)$ are each defined on $\{1,2,3\}$. Thus, the permutation p acted as follows:

$$p\colon \left\{ \begin{array}{l} 1 \longrightarrow 2 \\ 2 \longrightarrow 3 \\ 3 \longrightarrow 1 \end{array} \right\}$$

We also wrote this as

$$p: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

It is also convenient to adopt the notation

$$p(1) = 2$$

which is read "the image of 1 under p is 2," or "p takes 1 into 2" or " p at 1 is 2," or "p maps 1 onto 2," or "p of 1 equals 2." It also follows that

$$p(2) = 3 \text{ and } p(3) = 1.$$

The very same notation is used for q, r, s, t. Thus

$$r(1) = 1,\ r(2) = 3,\ r(3) = 2.$$

Observe that

$$p(p(1)) = p(2) = 3,\ p(r(2)) = p(3) = 1.$$

2 7 More Notation

You may recall that 7^2 means $7 \cdot 7$, that 7^3 means $7 \cdot 7 \cdot 7$. More generally, a^3 means $a \cdot a \cdot a$ and if n is a whole number greater than 1,

$$a^n = a \cdot a \cdot \ldots \cdot a$$

a is used as a factor n times.

As multiplication is associative, the grouping symbols have been omitted.

On the other hand, na may be interpreted to mean

$$na = a + a + \ldots + a$$

a is used an addend n times.

As addition is associative, the grouping symbols have been omitted.

When n = 0 and n = 1 we will agree to use

$$a^0 = 1 \quad \text{and} \quad a^1 = a,$$

While $$0 \cdot a = 0 \quad \text{and} \quad 1 \cdot a = a.$$

What interpretation can we give to p^2 for $(\{e,p,q,r,s,t\},o)$? As you may have guessed we take

$$p^2 = p \text{ o } p = q$$

Similarly $$p^3 = (p \text{ o } p) \text{ o } p = q \text{ o } p = e.$$

And in general if (S,o) is any operational system with just one operation, let us agree to the following meaning of a^n if $a \in S$:

$a^0 = e$, the identity element in (S,o) if it has one. If (S,o) has no identity, then a^0 names no element in S.

$$a^1 = a$$

$$a^2 = a^1 \text{ o } a^1$$

$$a^3 = a^2 \text{ o } a^1 = (a \text{ o } a) \text{ o } a$$

$$a^4 = a^3 \text{ o } a^1$$

....

$$a^n = a^{n-1} \text{ o } a^1$$

We must be careful about this convention. Suppose the system is $(Z_5,+)$. Then

2^3 means $2 + 2 + 2$ which is 1.

It could not mean $2 \cdot 2 \cdot 2$, because for this system the only operation we have is +. However, if the system is $(Z_5,\cdot)$. then

2^3 means $2 \cdot 2 \cdot 2$ which is 3. Hence, the meaning and value of 2^3 depends on the operational system in use. If a system has two binary operations $(S,+,\cdot)$ then we adopt the convention we have been using:

a^0 = identity element under $\cdot$ (if there is one)

$a^1 = a$

$a^2 = a \cdot a$

$a^3 = a^2 \cdot a = (a \cdot a) \cdot a$

$a^n = a^{n-1} \cdot a$

In other words, in the system $(S,+,\cdot)$ the value of a^n is the same as its value in the system $(S,\cdot)$. It should be very clear from the context exactly what is meant by a^n when we are dealing with a specific operational system.

2.8 Exercises

1. Tell whether each of the following mappings from $\{1,2,3,4,5\}$ into $\{1,2,3,4,5\}$ is 1-1, onto, and whether it is a permutation:

(a) $\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 & 4 \end{array}$

(b) $\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 & 5 \end{array}$

(c) $\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 3 & 2 & 1 \end{array}$

(d) $\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 4 & 3 & 5 \end{array}$

(e) $\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 4 & 3 & 4 \end{array}$

2. Tell whether each of the following mappings from Z into Z is 1-1, onto, and whether it is a permutation:

   (a) $f_1: n \longrightarrow n^2$

   (b) $f_2: n \longrightarrow 2n$

   (c) $f_3: n \longrightarrow n + 1$

   (d) $f_4: n \longrightarrow -n$

   *(e) $$f_5: \begin{cases} 0 \longrightarrow 0 \\ n \longrightarrow [\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n}] & \text{if } n > 0 \\ n \longrightarrow -[\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n}] & \text{if } n < 0 \end{cases}$$

   Note: [a] is the greatest integer not exceeding a.
   $[\frac{1}{2}] = 0$, $[4.9] = 4$, $[4] = 4$.

3. (a) For what domain and range will each of the mappings in Exercise 2 become onto mappings if they are not to begin with?

   (b) For what domain and range will each become mappings that are not onto if they happen to be onto?

4. Tell whether each of the following mappings from Q into Q is 1-1, onto, and whether it is a permutation:

   (a) $f_1: n \longrightarrow n^2$

   (b) $f_2: n \longrightarrow \frac{n}{2}$

   (c) $f_3: n \longrightarrow \frac{1}{n}$ for $n \neq 0$, $0 \longrightarrow 0$

   (d) $f_4: n \longrightarrow \left(\frac{1}{n^2 + 1}\right)$

   (e) $f_5: n \longrightarrow [n]$ ([n] is the greatest integer that does not exceed n -- see exercise 2.)

5. Using the definitions of f_1, f_2, f_3, f_4, and f_5 given in Exercise 4, compute:

(a) $f_1(\frac{2}{3})$

(b) $f_1(7.5)$

(c) $f_1(23.45)$

(d) $f_1(\frac{1}{2} \times \frac{3}{4})$

(e) $f_1(f_1(3))$

(f) $f_1(f_1(a))$

(g) $f_2(13)$

(h) $f_2(1.3)$

(i) $f_1(f_2(6))$

(j) $f_1(f_2(5))$

(k) $f_2(f_1(6))$

(l) $f_2(f_1(5))$

(m) $f_2(f_2(3.6))$

(n) $f_2(f_2(3.6))$

(o) $f_3(\frac{3}{7})$

(p) $f_3(1.25)$

(q) $f_3(f_3(\frac{3}{7}))$

(r) $f_3(f_3(1.25))$

(s) $f_3(f_1(7))$

(t) $f_1(f_3(7))$

(u) $f_4(f_3(7))$

6. Let the following mappings be from $Q\backslash\{0,1\}$ into Q:

$$f_1 : n \longrightarrow n$$

$$f_2 : n \longrightarrow 1 - n$$

$$f_3 : n \longrightarrow \frac{1}{n}$$

$$f_4 : n \longrightarrow \frac{1}{1-n}$$

$$f_5 : n \longrightarrow \frac{n}{n-1}$$

$$f_6 : n \longrightarrow \frac{n-1}{n}$$

Compute each of the following

(a) $f_1(5)$

(b) $f_2(5)$

(c) $f_3(5)$

(d) $f_4(5)$

(e) $f_5(5)$

(f) $f_6(5)$

(g) $f_2(f_2(5))$

(h) $f_3(f_3(5))$

(i) $f_4(f_6(5))$

(j) $f_5(f_5(5))$

(k) $f_6(f_4(5))$

(l) $f_2(f_6(5))$

(m) $f_6(f_2(5))$

(n) $f_3(f_4(5))$

(o) $f_4(f_3(5))$

(p) $f_2(f_3(5))$

(q) $f_3(f_2(5))$

(r) $f_4(f_4(5))$

*7. (a) Complete the composition table using the definitions in Exercise 6.

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1						
f_2						
f_3						
f_4						
f_5						
f_6						

Note: Interpret $(f_2 \circ f_3)(x)$ to be $f_3(f_2(x))$ here. For example $f_2 \circ f_3\ (n) = f_3(f_2(n)) = f_3(1-n) = \frac{1}{1-n}$ so that $f_2 \circ f_3 = f_4$.

(b) How does this table resemble the operation table for $(\{e,p,q,r,s,t\},\circ)$?

(c) Does the system $(\{f_1,f_2,f_3,f_4,f_5,f_6\},\circ)$ have the properties of a group?

(d) Compute $(f_3 \circ f_6)^I$.

8. Interpret and compute 3^2 for each of the following operational systems:

(a) $(Z_5,\cdot)$

(b) $(Z_5,+)$

(c) $(Z,+,\cdot)$

(d) $(Z_6,+)$

(e) $(Z_6,\cdot)$

(f) $(Z_6,+,\cdot)$

9. Using the definitions of Exercise 6, compute:

(a) $(f_4)^2\ (5)$

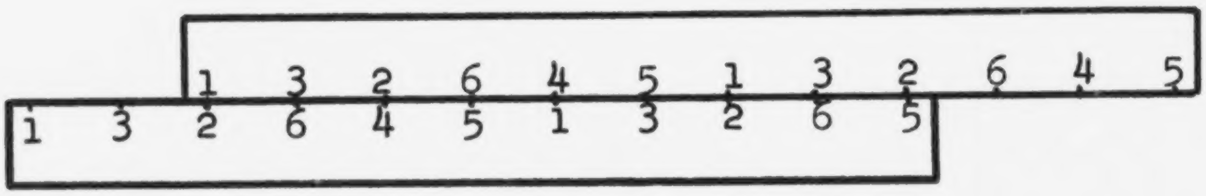
(b) $(f_4)^3\ (5)$

(c) $(f_5)^2\ (5)$

(d) $(f_6)^2\ (5)$

10. Express all the elements of the group $(Z_7\backslash\{0\},\cdot)$ as powers of 3. Is there another element in $Z_7\backslash\{0\}$ with the property that $\{t, t^2, t^3, t^4, t^5, t^6\} = Z_7\backslash\{0\}$?

11. A mechanical device can be constructed to compute in $(Z_7\backslash\{0\},\cdot)$. Corresponding to powers of 3, we use two peculiar rulers:



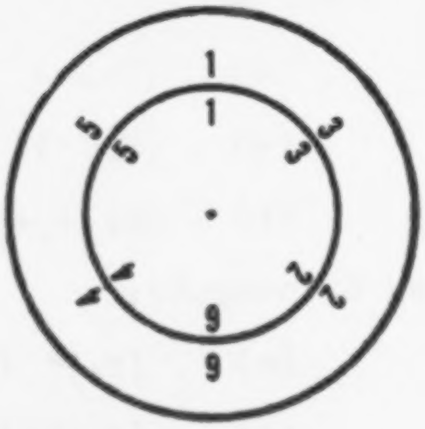
We have here 2 rulers with markings equally spaced and labeled as indicated The setting shown may be used to find $2\cdot x$ for any $x\in\{1,2,3,4,5,6\}$. Thus, under "5" of the upper scale we see "3" on the lower scale, telling us that

$$2\cdot 5 = 3.$$

Similarly, $2\cdot 6 = 5$, $2\cdot 4 = 1$, etc.

(a) Construct such a "slide rule" and compute $3\cdot 4$, $3\cdot 5$, $3\cdot 6$.

(b) Try to construct a "circular" slide rule that looks like this:



The central disc turns around its center while the disc in back may be held fixed.

12. Work Exercise 11 but use instead $(Z_{11}\backslash\{0\},\cdot)$ and powers of 2.

(a) Could you have used powers of 3?

(b) What other numbers could be used for our slide rule

(c) Check your slide rule by computing:

  (1) $7 \cdot 7$

  (2) $9 \cdot 5$

  (3) $4 \cdot 8$

  (4) $6 \cdot 10$

2.9 Some Theorems About Groups

In the previous sections we became aware of the existence of many groups. That is we saw many operational systems which have all the basic properties required of a group. We shall, in this section, deduce some consequences of the basic group properties which will therefore apply to all groups. Each consequence (or theorem) will then have an interpretation for every group; and in particular, the groups we have mentioned.

In what follows we shall assume that $\underline{a}$, $\underline{b}$, $\underline{c}$, $\underline{d}$ are arbitrary elements of some group (S, o) with e as its identity element.

Theorem 1. If $a = b$ then $a \circ c = b \circ c$.

We may refer to this theorem as "Right Operation."

Proof.

$a = b$	By assumption
$a \circ c = a \circ c$	Equality is reflexive
$a \circ c = b \circ c$	Substitution Principle of Equality $(a = b)$

As you might expect there is a companion theorem in which we have a "Left Operation."

Theorem 2. If $a = b$ then $c \circ a = c \circ b$.

We refer to this theorem as "Left Operation."

Proof	$a = b$	Assumption
	$c \circ a = c \circ a$	Equality is reflexive
	$c \circ a = c \circ b$	S. P. E. ($a = b$)

Theorems 1 and 2 will be used frequently in what follows, expecially in solving equations.

Whenever a mathematician establishes a theorem he invariably considers the possibility of a converse also being a theorem. The next two theorems are converses of Theorems 1 and 2.

Theorem 3. If $a \circ c = b \circ c$ then $a = b$.

We will refer to this theorem as "Right Cancellation."

Proof	$a \circ c = b \circ c$	Assumption
	$(a \circ c) \circ c^I = (b \circ c) \circ c^I$	Every element in a group has an inverse, and Right Operation.
	$a \circ (c \circ c^I) = b \circ (c \circ c^I)$	Associativity and S.P.E. $(a \circ c) \circ c^I = a \circ (c \circ c^I)$ $(b \circ c) \circ c^I = b \circ (c \circ c^I)$
	$a \circ e = b \circ e$	Definition of c^I and S.P.E. ($c \circ c^I = e$)
	$a = b$	Definition of e and S.P.E. ($a \circ e = a$, $b \circ e = b$)

Theorem 4. If $c \circ a = c \circ b$ then $a = b$.

We will refer to this theorem as "Left Cancellation."

Proof	$c \circ a = c \circ b$	Assumption
	$c^I \circ (c \circ a) = c^I \circ (c \circ b)$	Every element in a group has an inverse, and Left Operation.
	$(c^I \circ c) \circ a = (c^I \circ c) \circ b$	Associativity and S.P.E. $c^I \circ (c \circ a) = (c^I \circ c) \circ a$ $c^I \circ (c \circ b) = (c^I \circ c) \circ b$
	$e \circ a = e \circ b$	Definition of c^I and S.P.E. ($c^I \circ c = e$)
	$a = b$	Definition of e and S.P.E. ($e \circ a = a$, $e \circ b = b$)

Frequently, we shall not mention S.P.E. as a reason for a statement. It is hoped that you will be able to recognize that substitutions have been made and supply this part of the reason by yourself. Such omissions are common in mathematics and make for shorter proofs

Theorems 1, 2, 3, 4 are more frequently used than any others. Before proving any others let us see how they may be used to solve a variety of equations. If we look back to the beginning of this chapter, two equations were solved

$$3x = 12 \quad \text{and} \quad 3 + x = 12$$

We mentioned that through a study of groups these equations may be considered essentially of the same type. We are now in a position to show in what sense they are the same. We need one general result:

Theorem 5. If (S,o) is a group, and a and b are elements of S, then there is one and only one solution x in S of the equation $a \circ x = b$, and that is $x = a^I \circ b$.

Proof. Suppose there is an element $x \in S$ such that

$a \circ x = b$	Supposition
$a^I \circ (a \circ x) = a^I \circ b$	Left Operation
$(a^I \circ a) \circ x = a^I \circ b$	Associativity
$e \circ x = a^I \circ b$	Definition of a^I
$x = a^I \circ b$	Definition of e

We have shown that if there is an element $x \in S$ such that $a \circ x = b$, the only possible "value" for x is $a^I \circ b$; that is, there is at most one such element x. That $a^I \circ b$ has the desired property is easy to check, for if $x = a^I \circ b$, then

$a \circ x = a \circ (a^I \circ b)$	S.P.E.
$= (a \circ a^I) \circ b$	Associativity
$= e \circ b$	Definition of a^I
$= b$	Definition of e.

This shows that $a^I \circ b$ (which is an element of S) is the one and only solution x in S of $a \circ x = b$.

Returning to the problems $3 + x = 12$ and $3 \cdot x = 12$, we will deal with each as an application of Theorem 5 to a particular group. Theorem 5, as we proved, holds in all groups.

Since 3 and 12 are elements of the set Z, and since (Z,+) is a group (Exercise 17 of Section 2.2), we apply Theorem 5 to this case, and get that the equation $3 + x = 12$ has one and only one solution in Z, namely $x = 3^I + 12$. Since in (Z, +), $3^I = -3$, we have $x = (-3) + 12 = 9$.

Precisely the same solution applies in the second case. Since 3 and 12 are elements of $Q \setminus \{0\}$, and since $(Q \setminus \{0\}, \cdot)$ is a group (Exercise 17 of Section 2.2), there is one and only one solution x in $Q\setminus\{0\}$ of the equation $3\cdot x = 12$, namely $x = 3^I . 12$. Since $3^I = \frac{1}{3}$ in our group, $x = \frac{1}{3}.12 = 4$.

A slight change in the argument gives us

Theorem 6. If (S,o) is a group, and a and b are elements in S, then there is one and only one solution x in S of the equation $x \circ a = b$, and that is $x = b \circ a^I$.

Since the proof follows the pattern of proof in Theorem 5, we start it off, and leave it to you to complete it.

Proof. Suppose there is an element $x \in S$ such that

$x \circ a = b$	Supposition
$(x \circ a) \circ a^I = b \circ a^I$	Why?
$x \circ (a \circ a^I) = b \circ a^I$	Why?
$x \circ e = b \circ a^I$	Why?

Complete the proof, imitating the proof of Theorem 5.

The next two theorems may have been suggested to you in working out Exercise 1(d) in Section 2.4 For example, you should have observed that

$$(p^I)^I = p \quad \text{and} \quad (p \circ r)^I = r^I \circ p^I$$

while $$(p \circ r)^I \neq p^I \circ r^I.$$

These theorems will be proved by making use of the property that each element of a group has exactly one inverse. The method consists of proving that if x and y are both inverses of a, then x = y.

Theorem 7. For every element a in a group $(a^I)^I = a$.

Proof. We are going to show that $(a^I)^I$ and a are both inverses of a^I.

of $(a^I)^I$ is the inverse of a^I by the very meaning the symbol "$(a^I)^I$."

a is the inverse of a^I because $a^I \circ a = a \circ a^I = e$.

Since a^I has exactly one inverse, we conclude $(a^I)^I = a$.

Theorem 8. For every pair of elements a and b in a group $(a \circ b)^I = b^I \circ a^I$.

Proof. We shall show that $(a \circ b)^I$ and $b^I \circ a^I$ are inverses of the same element, namely, $(a \circ b)$. As each element of a group has exactly one inverse, it will then follow that $(a \circ b)^I = b^I \circ a^I$.

$(a \circ b)^I$ is the inverse of $(a \circ b)$ by definition of the symbol "$(a \circ b)^I$."

We now prove that $(b^I \circ a^I)$ is also the inverse of $(a \circ b)$.

$(b^I \circ a^I) \circ (a \circ b) = b^I \circ [a^I \circ (a \circ b)]$ Associativity

$= b^I \circ [(a^I \circ a) \circ b]$ Associativity

$= b^I \circ [e \circ b]$ Def. of a^I

$= b^I \circ b$ Def. of e

$= e$ Def. of b^I

Also:

$(a \circ b) \circ (b^I \circ a^I) = a \circ [b \circ (b^I \circ a^I)]$

Associativity

$= a \circ [(b \circ b^I) \circ a^I]$ Associativity

$= a \circ [e \circ a^I]$ Def. of b^I

$= a \circ a^I$ Def. of e

$= e$ Def. of a^I

As $a \circ b$ has exactly one inverse, and since $b^I \circ a^I$ and $(a \circ b)^I$ are inverses of $a \circ b$, we conclude $(a \circ b)^I = b^I \circ a^I$.

Let us give interpretations of this result in $(Z,+)$ and $(Q^+,\cdot)$.

Let $a = 2$ and $b = 3$ be elements of Z. Then $(a \circ b)^I$ becomes $-(2 + 3) = -5$ and $b^I \circ a^I$ become $(-3) + (-2) = -5$.

Let $a = 2$ and $b = 3$ be elements of Q^+. Then $(a \circ b)^I$ becomes $\frac{1}{2\cdot 3} = \frac{1}{6}$ and $b^I \circ a^I$ becomes $\frac{1}{3} \cdot \frac{1}{2} = \frac{1}{6}$.

In the exercises that follow, and hereafter, we shall say for brevity "a is an element of group (S,o)" or simply "a is an element of a group" to mean "a is an element of S, where (S,o) is a group."

2.10 Exercises

1. For the groups $(Z_7,+)$ and $(Z_7\setminus\{0\},\cdot)$ show that:
   (a) $(3^I)^I = 3$
   (b) $(3 + 4)^I = 4^I + 3^I$
   (c) $(3.4)^I = 4^I.3^I$
2. If a group is commutative (for every a and b, $a \circ b = b \circ a$) prove that $(a \circ b)^I = a^I \circ b^I$.
3. Prove the converse of Exercise 2, namely, if for

every a and b, $(a \circ b)^I = a^I \circ b^I$, then the group is commutative. [Hint: Let $x = a^I$, $y = b^I$. Then $y \circ x = b^I \circ a^I = (a \circ b)^I$.]

4. Supply the reasons for the following proof that $(a^I)^I = a$.

$$(a \circ a^I) \circ (a^I)^I = a \circ [a^I \circ (a^I)^I]$$

$$e \circ (a^I)^I = a \circ e$$

$$(a^I)^I = a$$

5. Supply the reasons for the following proof that $(a \circ b)^I = b^I \circ a^I$.

$$(a \circ b)^I = (a \circ b)^I$$

$$(a \circ b)^I \circ [(a \circ b) \circ (b^I \circ a^I)] = [(a \circ b)^I \circ (a \circ b)] \circ (b^I \circ a^I)$$

$$(a \circ b)^I \circ [\overline{(a \circ b) \circ b^I} \circ a^I] = e \circ (b^I \circ a^I)$$

$$(a \circ b)^I \circ [\overline{a \circ (b \circ b^I)} \circ a^I] = b^I \circ a^I$$

$$(a \circ b)^I \; [\overline{a \circ e} \circ a^I] = b^I \circ a^I$$

$$(a \circ b)^I \circ [a \circ a^I] = b^I \circ a^I$$

$$(a \circ b)^I \circ e = b^I \circ a^I$$

$$(a \circ b)^I = b^I \circ a^I$$

6. For the group $(\{e, p, q, r, s, t\}, \circ)$ in Section 2.3,

   (a) check that $(p \circ r)^I \neq p^I \circ r^I$.

   (b) check that $(p \circ r)^I = r^I \circ p^I$.

(c) find two other elements of the group which display the property indicated in (a) and (b).

7. Let (S, o) be a commutative group. Let $(S, \underline{o})$ be an operational system defined by: $a \ \underline{o} \ b = a \ o \ b^{I}$ for every a and b in S. Prove the following:

(a) $a \ \underline{o} \ a = e$

(b) $a \ \underline{o} \ e = a$

(c) $a \ \underline{o} \ a^{I} = a \ o \ a$

(d) If $a = b$ then $a \ \underline{o} \ c = b \ \underline{o} \ c$.

(e) If $a = b$ then $c \ \underline{o} \ a = c \ \underline{o} \ b$.

(f) If $a \ \underline{o} \ c = b \ \underline{o} \ c$ then $a = b$

(g) If $c \ \underline{o} \ a = c \ \underline{o} \ b$ then $a = b$

(h) $(a \ \underline{o} \ b) \ o \ b = a$

(i) $(a \ o \ b) \ \underline{o} \ b = a$

(j) $a \ o \ (b \ \underline{o} \ c) = (a \ o \ b) \ \underline{o} \ c$

(k) $a \ \underline{o} \ (b \ o \ c) = (a \ \underline{o} \ b) \ \underline{o} \ c$

(l) $(a \ \underline{o} \ c) \ o \ (c \ \underline{o} \ d) = a \ \underline{o} \ d$

(m) $(a \ \underline{o} \ b) \ o \ (c \ \underline{o} \ d) = (a \ o \ c) \ \underline{o} \ (b \ o \ d)$

(n) $(a \ \underline{o} \ b) \ \underline{o} \ (c \ \underline{o} \ d) = (a \ o \ d) \ \underline{o} \ (b \ o \ c)$

8. (a) Interpret each of the results in Exercise 7 if (S, o) is $(Z, +)$, $a = 0$, $b = 4$, $c = 5$, $d = 6$.

(b) Do the same if (S, o) is $(Q^{+}, \cdot)$, $a = 3$, $b = 4$, $c = 5$, $d = 6$.

2.11 Isomorphism

In looking at some of our operation tables you probably recognized a great similarity. Consider these examples.

Example 1.

+	Even	Odd
Even	Even	Odd
Odd	Odd	Even

x	Positive	Negative
Positive	Positive	Negative
Negative	Negative	Positive

$(Z_2,+)$

+	0	1
0	0	1
1	1	0

$(Z_3\backslash\{0\},\cdot)$

·	1	2
1	1	2
2	2	1

Example 2.

$(Z_4,+)$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(Z_5\backslash\{0\},\cdot)$

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Example 3.

$(Z,+)$, $(\{2^n : n \in Z\},\cdot)$

(See Section 2.2 Exercises 17 (a) and 18.)

In each example there is a code that "translates" each group into one of the other groups in that example. In Example 1 it is clear that the code could be:

$$+ \longleftrightarrow \cdot$$

$$0 \longleftrightarrow 1$$

$$1 \longleftrightarrow 2$$

meaning that if the symbols at the left +, 0, 1 are replaced in order by the symbols at the right · , 1, 2, then the table for $(Z_2,+)$ converts into the table for $(Z_3\backslash\{0\},\cdot)$. The replacement in the opposite direction converts the table for $(Z_3\backslash\{0\},\cdot)$ into the table for $(Z_2,+)$.

In Example 1, what is the code relating the odd-even group to $(Z_2,+)$?

In Example 2 the code is not as obvious. A rearrangement of columns and rows for one of the tables, say the second, will reveal the code. Thus

$(Z_4,+)$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(Z_5\backslash\{0\},\cdot)$

·	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

A code that serves to show that these groups are of the same type is:

$$+ \longleftrightarrow \cdot$$
$$0 \longleftrightarrow 1$$
$$1 \longleftrightarrow 2$$
$$2 \longleftrightarrow 4$$
$$3 \longleftrightarrow 3$$

In Example 3 the code seems to be

$$+ \longleftrightarrow \cdot$$

$$n \longleftrightarrow 2^n \text{ for each } n \in Z$$

where $2 = 1$, $2^{-1} = \frac{1}{2}$, $2^{-2} = \frac{1}{2^2} = \frac{1}{4}$, $2^{-3} = \frac{1}{2^3} = \frac{1}{8}$, etc.

A code is of little value if the "message" does not get through. We would like each "message" or expression in the coded text to translate "faithfully" into the original language. We will now try to indicate what we mean by "faithful" translation. In Example 3, let us consider a coded text, say

$$2^3 \cdot 2^4 \text{ which is } 2^{3+4} \text{ or } 2^7.$$

A translation of this message is

$$3 + 4 \text{ or } 7.$$

We may diagram this as follows:

$$\begin{tikzcd}
2^3 \arrow[d, leftrightarrow] & \cdot \arrow[d, leftrightarrow] & 2^4 \arrow[d, leftrightarrow] & = & 2^7 \arrow[d, leftrightarrow] \\
3 & + & 4 & = & 7
\end{tikzcd}$$

The notion of being a "faithful" code requires that the meaning of the message 2^7 and 7 should also correspond. In this case, 2^7 and 7 do correspond. In general, we have

$$\begin{tikzcd}
2^a \arrow[d, leftrightarrow] & \cdot \arrow[d, leftrightarrow] & 2^b \arrow[d, leftrightarrow] & = & 2^{a+b} \arrow[d, leftrightarrow] \\
a & + & b & = & a + b
\end{tikzcd}$$

for all a, b in Z. This guarantees faithful coding and decoding. When such faithful codes exist between two groups we call the groups isomorphic and the correspondence an isomorphism. More precisely we have this definition:

Definition. Let $(S, \circ)$ and $(S_1, \circ_1)$ be groups. A mapping f of S to S_1 is an isomorphism from (S, o) to (S_1, o_1) if and only if

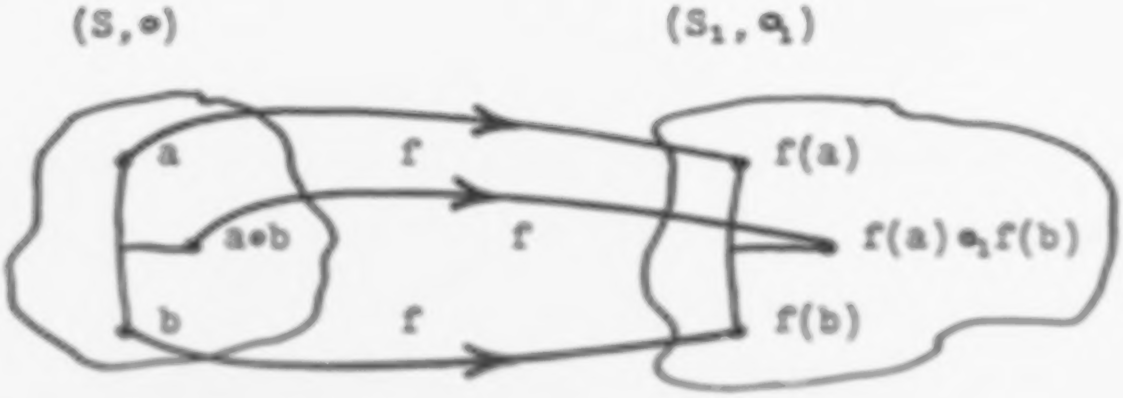
(1) f is 1-1 and onto.

(2) for every pair of elements a and b in S

$$f(a \circ b) = f(a) \circ_1 f(b).$$

The groups (S, o) and (S_1, o_1) are then said to be isomorphic.

We may picture an isomorphism as follows.



In Example 3 the mapping f defined by

$$n \longrightarrow 2^n$$

is an isomorphism from $(Z,+)$ to $(\{2^n: n \in Z\}, \cdot)$ because for each n there is exactly one image 2^n, different n's give different images, each 2^n is the image of some n, and for every pair of integers a, b in Z:

$$\begin{aligned} f(a + b) &= 2^{a + b} \\ &= 2^a . 2^b \\ &= f(a) \cdot f(b) \end{aligned}$$

The groups $(Z,+)$ and $(\{2^n: n \in Z\}, \cdot)$ are thus isomorphic.

When two groups are given, the problem of determining whether or not they are isomorphic may be very difficult. Not every 1-1 onto mapping f is an isomorphism between two groups.

The property (2), $f(a \circ b) = f(a) \circ_1 f(b)$ must be shown to hold. In some cases there may be two different mappings of the elements of one group into those of another, each of which is an isomorphism. In some of the exercises that follow you will be given two groups, and asked to find an isomorphism between them.

2.12 Exercises

1. Show that mapping f defined for every $n \in Z$ by

$$f: \quad n \longrightarrow 3^n \qquad \text{Where } 3^0 = 1,\ 3^{-1} = \frac{1}{3},\ 3^{-2} = \frac{1}{3^2} = \frac{1}{9},\ 3^{-3} = \frac{1}{3^3} = \frac{1}{27}, \text{ etc.}$$

   is a 1-1 mapping from the group $(Z,+)$ into the group $(Q\backslash\{0\},\cdot)$. Does it follow that $(Z,+)$ and $(Q\backslash\{0\},\cdot)$ are isomorphic groups? Why?

2. Show that the following groups are isomorphic:

   (a) $(Z_3,+)$ and

o	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

   (b) (The subsets of $\{a,b\}$,Δ) and (See Section 2.2, Ex. 14.)

o	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

   (c) $(Z,+)$ and $(\{3^n: n \in Z\},\cdot)$ (See Exercise 1. How can you show $(\{3^n: n \in Z\},\cdot)$ is a group?)

3. Show that the following groups are not isomorphic:

   (a) $(Z_4,+)$ and $(Z_6,+)$

*(b) $(Z_6,+)$ and $(\{e,p,q,r,s,t\},o)$

*(c) $(Z_4,+)$ and either group in Exercise 2(b)

*(d) $(Z,+)$ and $(Q,+)$

4. The order of a group (S, o) is the number of elements in S, if S is finite. The order of an element $a \in S$ is the smallest positive integer n for which $a^n = e$. Thus for the group $(Z_4,+)$ the order of the group is 4, while the order of the element 2 in $(Z_4,+)$ is 2.

   Find the order of each of the following groups and the order of each element in the group:

   (a) $(Z_4,+)$ (d) $(Z_7,+)$

   (b) $(Z_8,+)$

   (c) $(Z_6,+)$

2.13 Summary

1. A group is an operational system (S, o) such that:
   (1) For all a, b, c in S $(a \circ b) \circ c = a \circ (b \circ c)$. Associative Property.
   (2) There is exactly one element in S, e, such that for every $a \in S$, $a \circ e = e \circ a = a$. Identity Property.
   (3) For each $a \in S$ there is exactly one a^I in S, such that $a \circ a = a \circ a = e$. Inverse Property.
2. The permutation group $(\{e,p,q,r,s,t\},o)$ is an example of a non-commutative group.
3. The total number of arrangements of n objects in a row is $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot n$.

   In particular, the total number of arrangements of 4 objects, a, b, c, d, is 4! or 24.

4. If f is a mapping, f(a) is the image of a under this mapping.
5. If $a \in S$ and (S, o) is an operational system, a^3 means (a o a) o a.
6. If (S, o) and (S_1, o) are groups with S_1 a subset of S, then (S_1, o) is called a subgroup of (S, o).
7. A number of theorems were deduced for groups.

   If a = b then a o c = b o c and c o a = c o b.

   If a o c = b o c then a = b.

   If c o a = c o b then a = b.

   x o a = b and a o x = b have exactly one solution each, b o a^I and a^I o b respectively.

   $$(a^I)^I = a \quad (a \circ b)^I = b^I \circ a^I$$

8. A mapping f from group (S, o) into group (S_1, o_1) is an isomorphism if

   (1) f is 1-1 and onto.

   (2) f(a o b) = f(a) o_1 f(b) for all a, b in S.

   The groups (S, o) and (S_1, o_1) are then called isomorphic groups.

2.14 Review Exercises

1. Decide whether or not the following operational systems are groups
   - (a) $(Z_4, +)$
   - (b) $(Z_5 \backslash \{0\}, \cdot)$
   - (c) $(Z, \cdot)$
   - (d) $(Z^+, +)$

2. How many different arrangements in a row are there for the five letters a, b, c, d, e?

3. Compute:

   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}^I$

   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

4. Compute 3^2 for:

   (a) $(Z,+)$

   (b) $(Z_7,+)$

   (c) $(Z_7\backslash\{0\},\cdot)$

5. Find all the subgroups of $(Z_8,+)$.

   Does the definition of subgroup allow us to say that a group is a subgroup of itself?

6. Solve:

   (a) $t \circ x = p$ in $(\{e,p,q,r,s,t\},\circ)$.

   (b) $x \circ t = p$ in $(\{e,p,q,r,s,t\},\circ)$.

   (c) $(p \circ x) \circ t = q$ in $(\{e,p,q,r,s,t\},\circ)$.

   (d) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ ? & ? & ? & ? \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

7. Prove that the groups $(Z_6,+)$, $(Z_7\backslash\{0\},\cdot)$ are isomorphic.

8. Prove that for a, b, c in a group,

$$(a \circ x) \circ b = c$$

   has exactly one solution, $a^I \circ (c \circ b^I)$.

9. Prove that for a, b in a group,

   $(a \circ b^I)^I = b \circ a^I$.

10. Let P be a set of groups. "Is a subgroup of" is then a relation in this set. (Recall the definition of a relation from Course I.) Is this relation an equivalence relation? That is, is it reflexive, symmetric, and transitive?

11. Let $(S, \circ)$ be an operational system with the associative property, the identity property, and the additional property that for any $a, b \in S$, each of the equations

$$a \circ x = b \text{ and } y \circ a = b$$

has a unique solution in S. Prove that $(S, \circ)$ is a group. Hint: If e is the identity element, and $\underline{a}$ is any element in S, and $\underline{x}$, $\underline{y}$ the respective solutions of $a \circ x = e$ and $y \circ a = e$, it is sufficient to prove $x = y$. (Why?) Then start with $(y \circ a) \circ x = y \circ (a \circ x)$.

CHAPTER 3

AN INTRODUCTION TO AXIOMATIC AFFINE GEOMETRY

3.1 Preliminary Remarks

In this course, there have been a number of occasions when we deduced theorems from axioms. For example, in the chapter on Elementary Number Theory (Course I, Chapter 11) we derived important divisibility properties of natural numbers by listing some axioms for $(N,+,\cdot)$ and then proceeding to reason in a logical fashion from these axioms. Similarly, in Chapter 2 on Group Theory we deduced some important theorems about groups, using the associative, identity and inverse properties as axioms. The logical ideas used in carrying out deductions, such as these, were analyzed and discussed in Chapter 1 on Proof.

In this chapter once again we develop a deductive system. We shall begin with some familiar words like *plane*, *line*, and *point*. However, instead of trying to define what these things are, we shall merely stipulate that they obey certain axioms. The axioms or assumptions about these objects will state a few significant properties already familiar from experience. Our task will be to show that a number of other properties of points, lines, and planes follow by deduction from the assumptions.

Since the axioms are suggested by our experience with points, lines, and planes, whatever can be deduced from the axioms should also correspond with experience. However, we are limiting the number of properties to be used as axioms. Therefore there will be properties of lines and points which cannot be deduced from the limited number of axioms we will adopt. Although we will be dealing with objects called points, lines, and planes, we will not make use of any properties of these objects except those stated precisely in the axioms.

3.2 Axioms

We shall limit our discussion to the points and lines of a single plane which will be denoted by π (the Greek letter Pi). If you insist upon thinking of this plane as a flat surface like a floor, you may do so. However, the only real requirement imposed upon this plane is that it is a set of points which satisfies the axioms stated below.

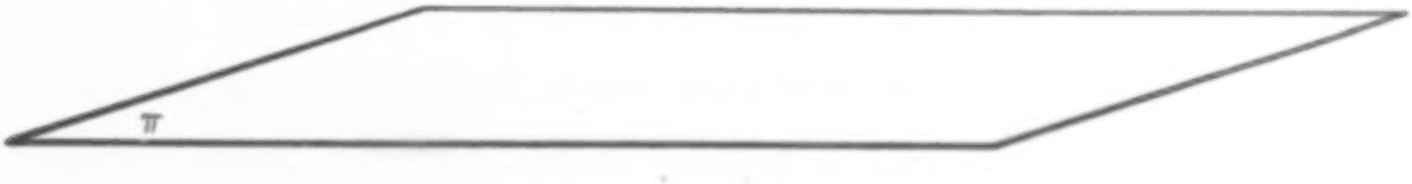


Figure 3.1

A Picture of a Plane

We will focus attention on certain subsets of the plane which have special properties.

Among these subsets are the lines (straight lines) of the plane. Again, if you insist upon thinking of a line as a taut wire, you may do so. We only insist that the line possess the properties which will be mentioned in the axioms.

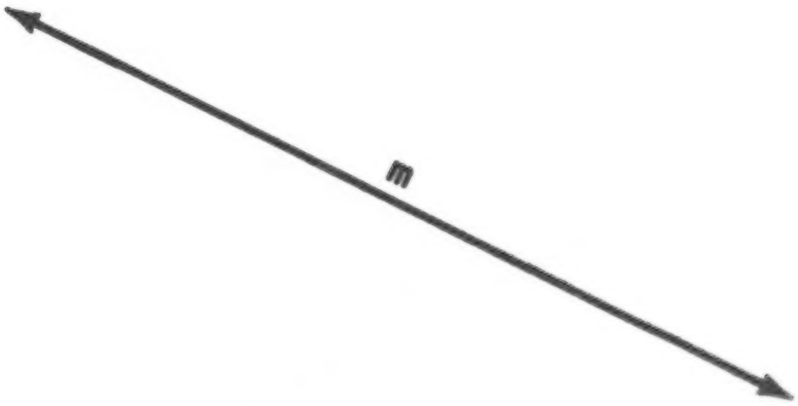


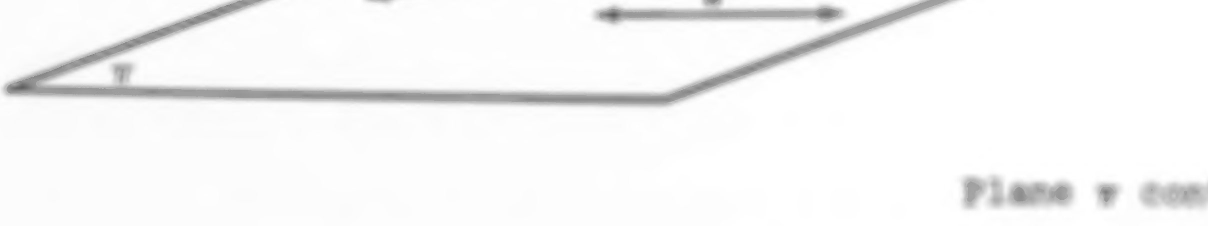
Figure 3.2

A Picture of a Line

The first axiom is given in two parts. In the first place, it requires that the plane contain at least two lines. A plane with only one line in it would hardly be much of a plane. The axiom also requires that each line contain at least two points. This certainly seems like a reasonable requirement. In fact, you probably feel that lines ought to have infinitely many points; we will not demand quite this much at present.

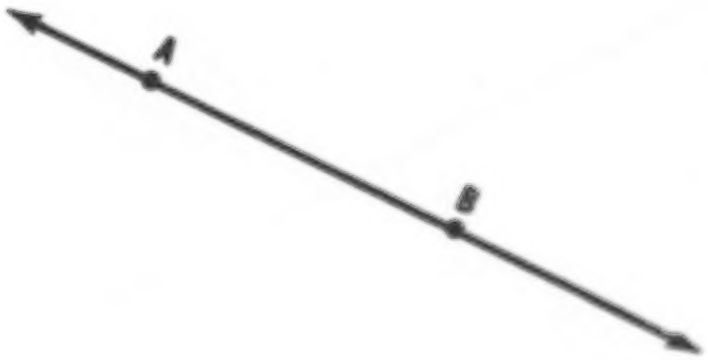
Axiom 1. (a) Plane π is a set of points, and it contains at least two lines.

(b) Each line in plane π is a set of points containing at least two points.



Plane π contains at least two lines.

Figure 3.3 (a)



Each line contains
at least two points.

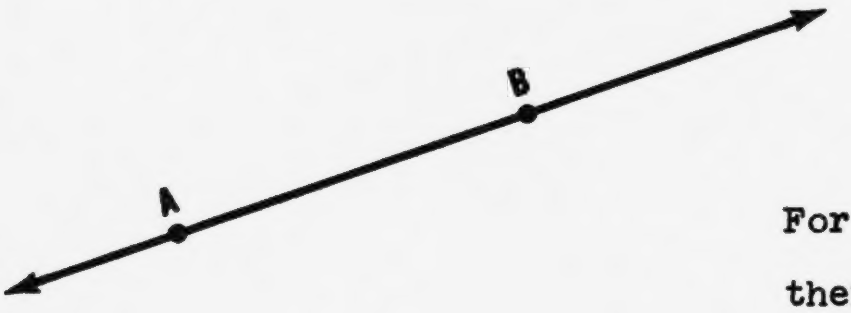
Figure 3.3 (b)

A Picture for Axiom 1

The second axiom also expresses a property that is reasonable to expect of lines and points. You will see that it plays an important part in our reasoning.

If someone were to ask you how many straight lines there were containing one particular point of a plane, you would probably say, "As many as you want." But if you were asked how many straight lines there were containing two different points, you would undoubtedly agree, "Just one." Certainly, whenever you draw a straight line through two points, A and B, you feel that there should be just one line, even though your drawing might not be accurate. At present we are not concerned about drawings. We are concerned only with ideas. The second axiom expresses a conviction about points and lines that you probably already have.

Axiom 2. For every two points in plane π there is one and only one line in π containing them.



For every two points
there is one and only
one line containing them.

Figure 3.4

A Picture for Axiom 2

When we say "two points" we shall always mean two distinct points. When we say "two lines " we shall mean two distinct lines. On the other hand when we say "lines m and n (without using "two") we shall allow the possibility that "m" and "n" name the same line.

Our third axiom deals with parallel lines. After we state it below, you will probably agree that it is a very reasonable requirement. In fact, for two thousand years this axiom appeared so reasonable that many of the finest mathematicians thought that it was unnecessary to assume it. They felt that it should be possible to prove this particular property from the other axioms which had been adopted for Geometry. In other words, they thought that it ought to be a theorem rather than an additional axiom.

Before we state this axiom we should be clear about what we mean by "parallel lines." When we draw two lines, call them "m" and "n," on a sheet of paper, they may appear to intersect, as in Figure 3.5;

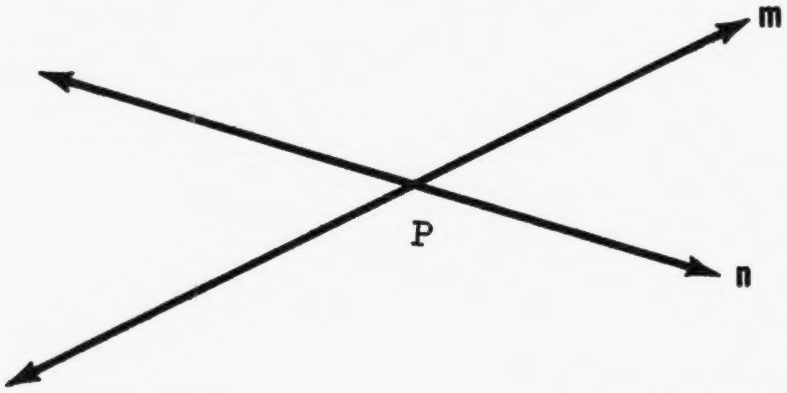


Figure 3.5

A Picture of Intersecting Lines

or they may appear not to intersect, as in Figure 3.6.

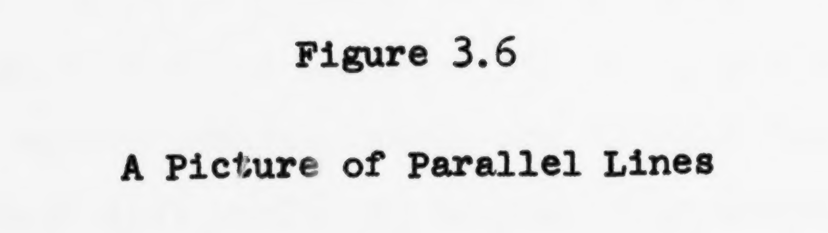


Figure 3.6

A Picture of Parallel Lines

Of course, in the second case it is possible that m and n really do intersect. Perhaps if each line were extended sufficiently far beyond the confines of our sheet of paper, we would see that they actually meet. On the other hand, it might be difficult or perhaps impossible to decide this question in some cases. We certainly can conceive that lines m and n might never intersect; that is $m \cap n = \emptyset$. In such a case we call lines m and n parallel. It is convenient as you will see to consider a line to be parallel to itself. Accordingly, let us state the following definition.

Definition 1. Lines m and n in π are said to be parallel if $m = n$ or if $m \cap n = \emptyset$. When lines m and n are parallel, we express this fact by writing "$m \parallel n$."

Our third axiom can now be stated.

Axiom 3. For every line m and point E in the plane π, there is one and only one line in π containing E and parallel to m.

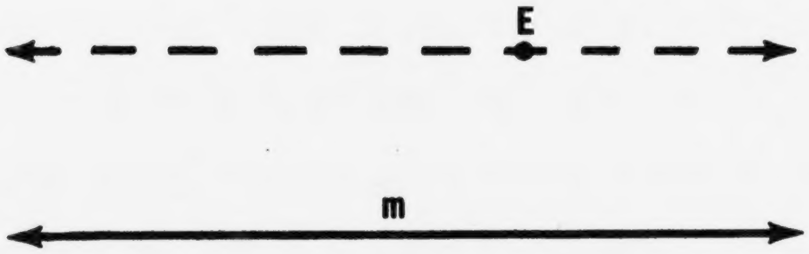


Figure 3.7

A Picture for Axiom 3

The need for such an axiom dealing with parallel lines was first recognized by Euclid who lived during the third century B.C. The axiom he adopted was the fifth in his list of axioms for geometry, and it corresponds closely to the one we have introduced here as our third axiom. The choice of this assumption was one of Euclid's great accomplishments for as we have noted, mathematicians for thousands of years after Euclid tried in vain to deduce this reasonable property from the other axioms.

That all these efforts were destined to failure was proved in the nineteenth century when a number of great mathematicians (Gauss, Bolyai, Lobachevsky) showed that Euclid's fifth axiom did not follow from his other axioms. They proved this by creating perfectly good systems of geometry which did not have the property demanded by that axiom. Such systems are called non-Euclidean Geometries. If a system of geometry includes Euclid's fifth axiom, or any axiom equivalent to it, then that axiom is referred to as the Euclidean Axiom in the system.

Before proceeding further, let us pause to examine our three axioms and our definition of parallel lines. We must not only be very clear about what these axioms and definition actually say -- we must be equally clear about what they do not say!

Axioms 1 and 2 express the idea that a certain set called a plane contains as subsets other sets called lines and that these lines contain points. The idea that a point is contained in a line, a line in a plane, etc. is called an incidence relation. Hence Axioms 1 and 2 are often called Incidence Axioms. Axiom 3, deals with another relation, namely parallelism. A system of geometry in which our Axioms 1, 2 and 3 hold is called an affine geometry.

Let us look again at Axiom 1. It asserts that the plane π contains at least two lines, and that each line in π contains at least two points. You may feel that a plane ought to contain more than two lines, perhaps infinitely many, and similarly a line should contain more than two points. Nevertheless, you must admit that Axiom 1 does not assert either of these possibilities, nor does it deny either of these possibilities. As far as Axiom 1 is concerned, the plane π may or may not contain more than two lines. Similarly, neither Axiom 2 by itself, nor Axiom 3 by itself, tells us how many lines there are in the plane, nor how many points there are in a line. We must keep an open mind on such matters. We must agree that we will accept only what is asserted by our axioms and definitions.

In Section 3.4 we shall study some statements that can be deduced logically from our axioms and definitions. Meanwhile you must try not to read into them any more than they actually say. The following exercises will test your understanding of this important point.

3.3 Exercises

1. (a) According to our definition of parallel lines, if line m is parallel to line n, can m and n have points in common? Explain.
   (b) If m || n does it follow that n || m?
2. If point E is contained in line m of plane π, is there a line containing E and parallel to m?
3. Which axiom, if any, asserts that a line can contain three points?
4. Which axiom, if any, asserts that there are more than two lines in plane π, containing any given point of π?
5. Which axiom if any, implies that each line in π contains at least one point?
6. Which axiom, if any, implies that given two distinct points, there cannot be two distinct lines, each containing both of these points?

7. Which axiom, if any, asserts that given two distinct lines, there is one and only one point contained in both of these lines?
8. Axiom 1 asserts that plane π contains at least two lines and that each of these lines contains at least two points. From the fact that the first line contains two distinct points and the second line also contains two distinct points can we logically conclude that there are at least four distinct points in plane π? (After all doesn't 2 + 2 = 4?) Explain.
9. Can two (distinct) lines intersect in two (distinct) points? Explain your answer by referring to the appropriate axiom or axioms.

*10. Using Axioms 1 and 2 only, give a logical argument to show that there are at least three points in plane π.

3.4 Some Logical Consequences of the Axioms

Statements which can be deduced logically from axioms are called theorems. As an example of a theorem which we can deduce fairly simply from our incidence axioms, consider the statement:

> If m is a line in plane π, then there is a point in π which is not in m.

Notice that no one of our axioms actually asserts this fact. Let us see what light Axiom 1 can throw on the situation. Since m is a line in plane π, Axiom 1(a) assures us that there is at least one other line besides m in plane π. Let us call such another line n. Now Axiom 1(b) assures us that each of the lines m and n contains at least two distinct points. We are seeking a point not in line m, so we consider two points that are in line

n. Let us call these points A and B. Our search will be ended if we can prove that at least one of these two points, A or B, is not in line m. Axiom 2 has something to say about this matter. Axiom 2 asserts that there can be only one line containing the two distinct points A and B. Therefore, since these two points were chosen in line n to start with, they cannot both also be in line m. At least one of them is therefore not in line m and that is what we wanted to prove.

We have spelled out the proof of our first theorem in considerable detail because we wanted to point out to what extent each axiom helped in the proof. It is customary to present a theorem and its proof in somewhat briefer form.

For example our first theorem might be displayed as follows:

Theorem 1. If m is a line in π then there is a point in π which is not in m.

Proof. By Axiom 1(a) there is a line n distinct from the given line m; that is, $m \neq n$. By Axiom 1(b) there are distinct points A and B in n; that is, $A \neq B$. If both A and B were in m, then by Axiom 2 we would have $n = m$, which is not the case. Hence at least one of the points A or B is not in m.

You may have noticed that we proved Theorem 1 without drawing any diagrams. Perhaps it seems a bit queer that we should make statements about points and lines without even drawing a figure to picture these points and lines. Actually, we did so on purpose. We wanted to emphasize the fact that our proof depends solely on the axioms. When we draw diagrams, there is always the danger that we might use in our reasoning some property of the diagram which really does not follow from the axioms. For example, when we draw a line as in Figure 3.8

Figure 3.8

it appears to contain very many points -- surely more than two! However, Axiom 1 merely tells us that there are at least two points in each line, and we have no right to assume that there are actually more than two just because it looks that way in the drawing.

Does this imply we must always avoid drawing a figure? We shall make no such rule! A diagram can often be a great help in suggesting important or useful relationships and it can frequently serve to guide us when things get complicated or when it is difficult to see what should come next. We should not hesitate to use a diagram in such cases but we should be very careful to avoid introducing into our reasoning any properties of the diagram which we cannot deduce from our axioms and definitions.

To help you capture the spirit of the deductive method let us prove another simple incidence theorem in full detail. When we are finished, we shall then display the theorem and its proof more briefly as we did with Theorem 1. Consider the statement:

> There are at least three points in plane π which are not all contained in the same line.

Notice again, that none of our axioms actually makes this assertion. Axiom 1(b) asserts that there are at least two points in every line of π, and Axiom 1(a) guarantees that there are at least two lines in π. Let us therefore select one of these lines, call it m. We know there are at least two points, call them A and B, in line m. The two points A and B are surely contained in plane π since line m is contained in π. The situation thus far may be pictured as in Figure 3.9.

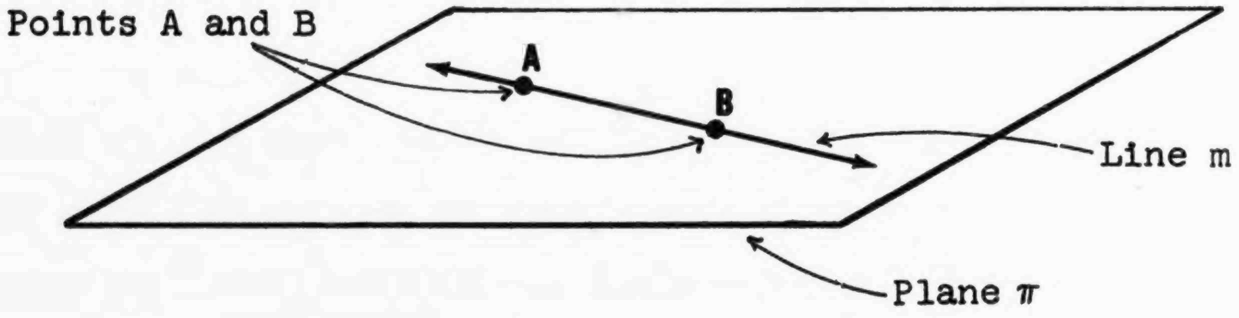


Figure 3.9

We still need to prove that there is, in plane π, a third point that is not in line m. But that is easy because we have already proved Theorem 1 which states that if m is a line in π, then there is a point in π which is not in m. Since Theorem 1 was deduced solely from the axioms, we may use Theorem 1 in our reasoning. We conclude that there is, in plane π, a point C which is not in line m:

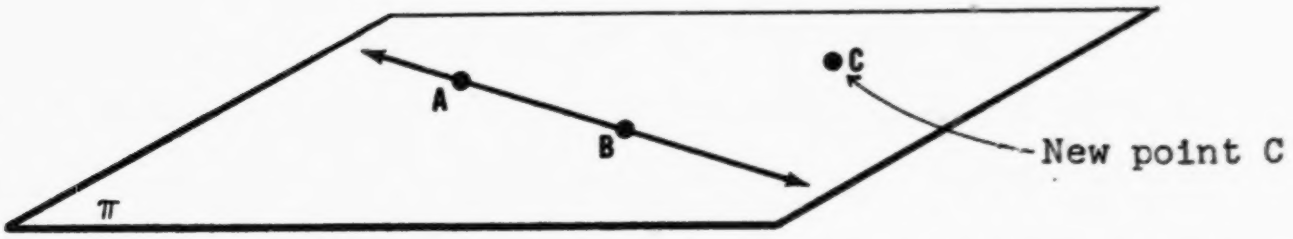


Figure 3.10

Because line m is the only line containing A and B (Axiom 2), and the point C is not in line m, it follows that C must be distinct from A and B. We have therefore proved that there are at least three points in plane π, which are not all contained in the same line.

Before we restate this theorem and others like it, it will be convenient to introduce a single word to express the idea that three (or more) points are contained in the same line. We call such points collinear.

Definition 2. (a) A set of points is called collinear, if there is a line containing all of them.

(b) A set of points is called non-collinear, if there is no line containing all of them.

We can now restate our second theorem more compactly and summarize its proof.

Theorem 2. There are at least three non-collinear points in plane π.

Proof. By Axiom 1(a), π contains at least two lines. Let m denote one of these lines. By Axiom 1(b), m contains at least two points, A and B. By Theorem 1, there is a point C in π which is not in m. This point C must be different from either A or B because by Axiom 2 m is the only line containing A and B, and C is not in m. Thus π contains (at least) the three non-collinear points A, B, and C.

For later use (see e.g. Exercise 4 below) we shall find it convenient to introduce a single word to describe three (or more) lines which have a point in common. We call such lines concurrent.

Definition 3. (a) Three (or more) lines in π are called concurrent if there is a point in π which is contained in all of them.

(b) Three lines in π are called non-concurrent, if there is no point in π which is contained in all of them.

Now try your skill at proving a few theorems by yourself. You may draw diagrams if you wish, but remember to base your reasoning solely on the axioms, definitions and theorems previously deduced.

3.5 Exercises

Prove each of the following theorems.

(Note: In the first two exercises we will suggest statements for the proof and ask you to justify these statements, i.e. to cite the appropriate axiom or theorem. After you complete these two exercises, you are on your own.)

1. (Theorem 3) Two (distinct) lines in plane π cannot have more than one point in common.

Proof

Let m and n be any two distinct lines in π.	Question: Which axiom guarantees that there are such lines in π?
Let A and B be any two points in m.	Which axiom guarantees that there are two such points in m?
Line m is the only line containing A and B.	Which axiom applies here?

Since line n is distinct from m, n cannot also contain both A and B. This means that n cannot have more than one point in common with m.

2. (Theorem 4) If A is a point in plane π, there is a line in π which does not contain A.

Proof (Supply reasons). There are at least two lines in plane π. (Why?) Call these lines m and n. If either of these lines does not contain A, there is nothing more to prove. On the other hand if both m and n contain A, then each of these lines must contain an additional point. (Why?) Call these points B and C. Since m and n are distinct lines, B and C must be distinct points. (Why?) There must therefore be a line containing B and C. (Why?) This line does not contain A. (Why?)

3. (Theorem 5) If A is a point in plane π, there are at least two lines in π each containing point A.
4. (Theorem 6) There are at least three non-concurrent lines in π. (Note: Refer to Definition 3(b) above.)
5. (Theorem 7) If each of two lines in π is parallel to the same line in π, then they are parallel to each other.
6. (Theorem 8) If m is any line in plane π, then there are at least two points in π which are not in line m. (Hint: You will need to use Axiom 3 in your proof.)

*7. (Theorem 9) If A is any point in plane π, then there are at least two lines in π which do not contain A.

8. (Theorem 10) If ℓ, m and n are lines in π such that m is parallel to n, then if ℓ is not parallel to m, it follows that ℓ is not parallel to n.

*9. (Theorem 11) If ℓ is any line in plane π and A is any point in π which is not in line ℓ, then there is a one-to-one correspondence between the set of all points in ℓ, and the set of all lines in π which contain A and are not parallel to ℓ.

*10. (Theorem 12) If A is any point in plane π, then there are at least three distinct lines in π each containing A.

3.6 A Non-Geometric Model of the Axioms

An army captain wishes to set up and train a commando squad from which he will select teams to go out on various dangerous missions. It will be necessary to have available at least two teams for various missions in the future. For each mission he will need a team of at least two trained commandos. It is desirable that each man in the commando squad be trained to work smoothly with any of the other men, so the captain orders that every two commandos must serve together in exactly one team. Moreover since any one of the teams might be out on a mission at any given time, the captain rules that for each of the remaining commandos there must be exactly one completely distinct team available to which this commando belongs.

We expect that as you were reading the above paragraph you were wondering what all this had to do with geometry! What do commando teams going out on dangerous missions have to do with points, lines, planes and axioms? Let us go over the above paragraph once more and summarize the requirements the captain has laid down:

1. (a) The commando squad is a set of commandos, and it must contain at least two teams.
   (b) Each team in the squad is a set of commandos and it must contain at least two commandos.
2. For every two commandos in the squad there must be one and only one team (exactly one team) in the squad to which they both belong.
3. For every team in the squad, and for each commando in the squad, but not in the team, there must be one and

only one (exactly one) completely distinct team in the squad to which the commando belongs.

As you read this summary doesn't it sound a bit familiar? Let us compare these requirements with our axioms for points and lines in the plane π. The first of these was:

Axiom 1. (a) Plane π is a set of points, and it contains at least two lines.

(b) Each line in plane π is a set of points containing at least two points.

The similarity between this axiom and the captain's first requirement is indeed striking! If we merely replace three terms:

"plane π" by "the commando squad"
"line" by "team"
"point" by "commando"

then Axiom 1 turns precisely into the statements which express the captain's first requirement above.

Now let us make these very same replacements in the next axiom for points, lines and plane π.

Axiom 2. For every two points in plane π there is one and only one line in π containing them.

After such replacement we obtain:

For every two commandos in the commando squad, there is one and only one team in the squad containing them.

This expresses precisely the captain's second requirement.

Next, let us look at the captain's third requirement:

For every team in the commando squad and for each commando in the squad, but not in the team, there must be one and only one completely distinct team to which the commando belongs.

Let us replace the underlined words by their counterparts listed above getting:

For every line in plane π and for each point in π but not in that line there must be one and only one completely distinct line in π to which the point belongs.

You will recognize that this statement is essentially the same as our geometric Axiom 3. The phrase "completely distinct line" refers now to a line that has no points in common with the original line. In Definition 1 we defined such a line to be parallel to the original line. If we had so desired we could have defined two completely distinct teams to be parallel teams and also agreed to call any team parallel to itself. In that case we would have expressed the captain's third requirement in a manner analogous to the way we expressed Axiom 3.

Now you may still feel that what we are doing here appears somewhat peculiar. Isn't it silly to replace well established words like "point" and "line" by other words such as "commando" and "team," which really have completely different meanings? This question deserves an answer and it merits a bit of careful discussion.

Let us look back again at how we have used the familiar words "point," "line" and "plane" in this chapter. We have taken great pains to emphasize the idea that in a deductive system we agree to accept only our axioms and what we can deduce logically from them. Although our axioms refer to points, lines, and planes, we have tried to be very careful (especially when referring to diagrams of these items) not to use any information about points, lines and planes that does not follow logically from the axioms.

Because of this point of view, we made no attempt to define the words point, line or plane. We required merely that they obey Axioms 1, 2 and 3. Since these are the only requirements we have laid down thus far, it is perfectly logical to interpret the words point, line and plane to mean any objects and sets of objects which satisfy the requirements laid down by our axioms. If the requirements imposed by the captain on his commandos, his teams of commandos, and the commando squad are exactly the requirements which our axioms imposed on points, lines, and planes, then it is not at all silly to re-interpret one set of words in terms of another. On the contrary, we can often learn a great deal in this way by using what we know about one system of objects to shed light on another system.

As a simple example of how useful it can be to interpret our geometric ideas in non-geometric terms, let us look at some of the theorems we have deduced from our axioms.

Theorem 3 asserted:

> Two (distinct) lines in plane π cannot have
> more than one point in common.

If we replace: "plane π" by "the commando squad"
"line" by "team"
"point" by "commando"

this theorem becomes:

> Two (distinct) teams in the commando squad
> cannot have more than one commando in common.

Although the captain did not list this restriction among his requirements, it is important that he realize that this restriction is implied by his requirements. The theorem tells him that in forming his teams he must avoid assigning the same two commandos to two different teams. Failure to understand this point would either make it impossible for him to meet his requirements or cause him to waste a great deal of time assigning and then re-assigning his men by trial and error.

Other rules which the captain must follow, and pitfalls which he must avoid, are illustrated by Theorems 5 and 9. Translating these theorems into the language of commandos, teams, etc. Theorem 5 asserts:

> If A is a commando in the commando squad then there are at least two teams in the squad each containing that commando.

In other words:

> Each commando must belong to at least two teams.

Similarly, Theorem 9 asserts:

> For each commando, there must be at least two teams to which he does not belong.

You should verify each of these rules by "translating" Theorems 5 and 9 from the "point" and "line" language to the "commando" and "team" terminology. The exercises below will indicate further results which can be obtained in this way.

3.7 Exercises

1. Interpret ("translate") Theorems 1 and 2 in terms of commandos and teams.
2. By translating Theorem 4, show that no commando in the squad can be a member of all the teams.
3. Would it be possible for the captain to set up his teams so that any three teams share at least one commando? (Which theorem or axiom sheds light on this?)
4. By interpreting the appropriate theorem, show that no matter which team is selected, there will always be at least two commandos in the squad who are not assigned to that team.
5. By interpreting Theorem 10, show that if two teams have no members in common, then any team that has a commando in common with one of these two teams, must share a commando with the other team also.

*6. Show that the number of teams to which any commando in the squad belongs must be one greater than the number of commandos in any team to which he does not belong. (Hint: Refer to Theorem 11.)

7. Suppose the captain selects three men, Jones, Kelly and Levy as his commando squad and forms three teams as follows:

   Team 1: {Jones, Kelly}
   Team 2: {Jones, Levy}
   Team 3: {Kelly, Levy}

   Does this arrangement satisfy all of his requirements? If not, which requirement is not satisfied and why?

8. Suppose the captain adds an additional commando to the squad (in Exercise 7) so that the commando squad now consists of four men:

   Jones, Kelly, Levy and Mason.

   Arrange these four commandos into teams in such a way that all the axioms, i.e., all the captain's requirements, are satisfied.

9. (a) Prove (Theorem 13): There are at least four points in plane π, no three of which are collinear.

   (b) Interpret this theorem in relation in Exercises 7 and 8.

3.8 Other Models of the Axioms -- Finite and Infinite

The somewhat unorthodox interpretation of our "geometry" axioms in terms of commandos, teams, etc. is an example of a *model* for these axioms. In this section we shall study a number of other interesting models that can be constructed by giving various interpretations to the words *point*, *line*, *plane* π, and the incidence relations involving points, lines and the plane π.

Four "Point" Models

I. Four businessmen, Mr. Adams, Mr. Brown, Mr. Crane and Mr. Drake get together to form a corporation. They invest in six different business enterprises and agree to share equally in the management of these enterprises. To do this they agree to set up two-man boards of directors to supervise the enterprises, a different two-man board for each. The corporation and its various boards of directors can be pictured as in Figure 3.11.

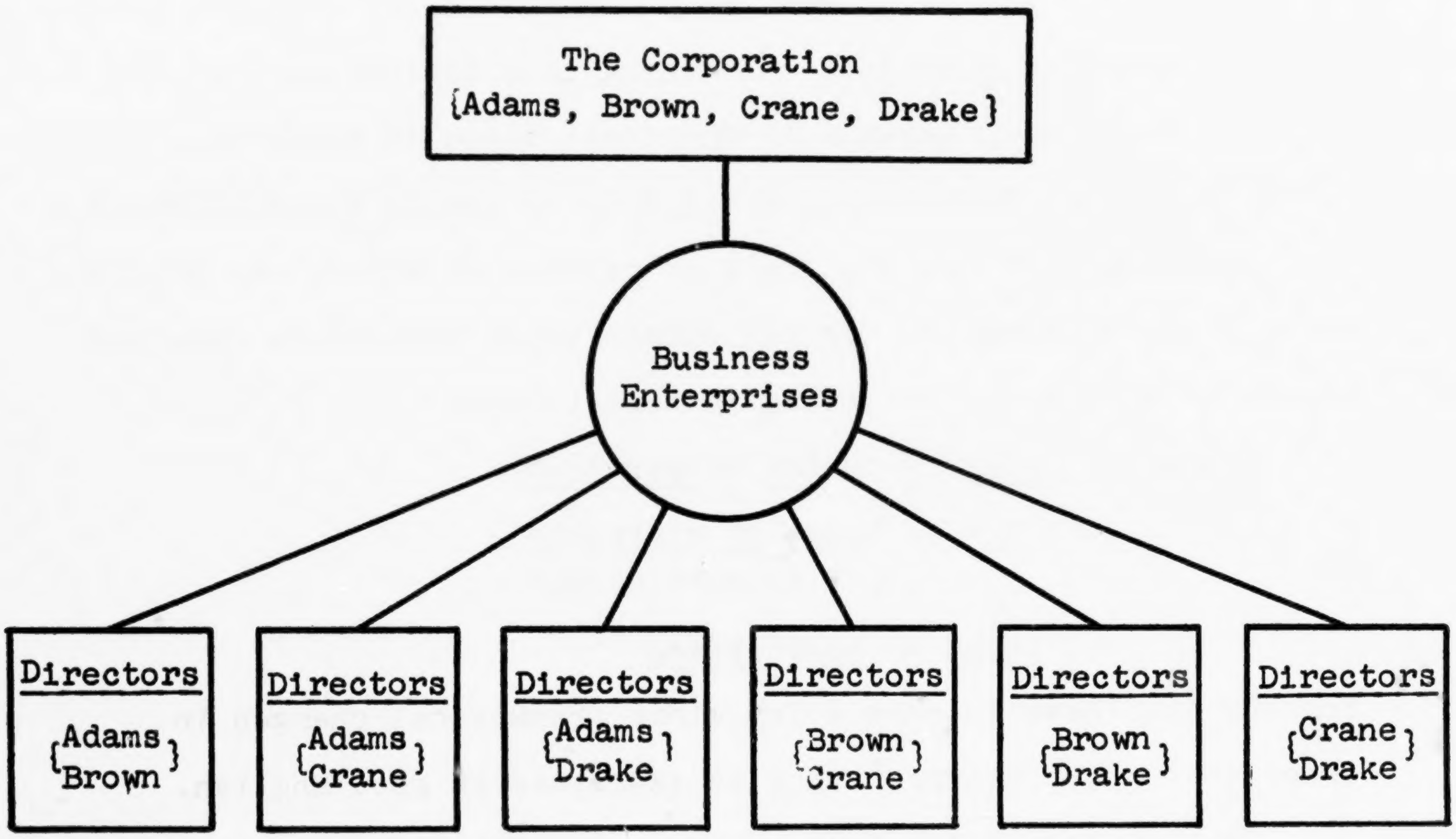

The Corporation
{Adams, Brown, Crane, Drake}
Business Enterprises
Directors
{Adams Brown}
Directors
{Adams Crane}
Directors
{Adams Drake}
Directors
{Brown Crane}
Directors
{Brown Drake}
Directors
{Crane Drake}

Figure 3.11

To see that this corporate structure is indeed a model for our axioms let us observe the following:

1. (a) The corporation is a set of businessmen, and it has at least two boards of directors (that manage enterprises owned by the corporation).
   (b) Each board of directors includes at least two of the business men -- in fact exactly two.
2. For every two business men in the corporation there is one and only one board of directors containing these two men.

3. For each board of directors of one of the enterprises and each businessman in the corporation who is not in this board of directors, there is one and only one other board of directors containing this businessman but not containing any man in the first board of directors. (Note: You should verify this by taking specific cases.)

Once again we see the familiar pattern of our axioms exhibited in these statements. We can obtain these statements from our axioms by making the following interpretations:

Replace: plane π by the corporation
line by board of directors
(of an enterprise)
point by businessman

You may also have to make a few minor grammatical changes in order that your interpretation be expressed in good English.

The pairing of the four business men into the six boards of directors might be conveniently pictured as in Figure 3.12.

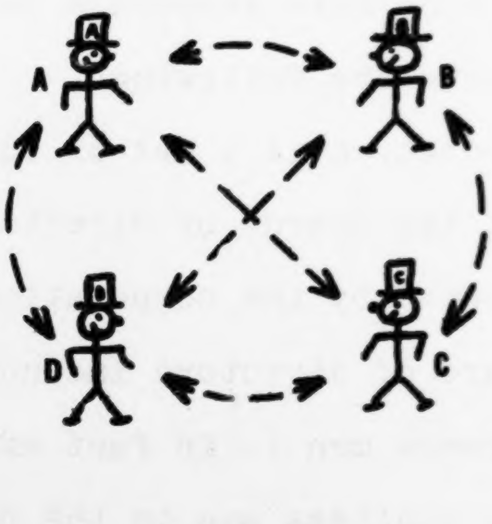


Figure 3.12

II. In Figure 3.12, each of the six double headed arrows indicates one of the six boards of directors. An even simpler diagram results if we use a dot (point) to represent each businessman and a segment connecting each pair of dots to indicate each of the directorships.

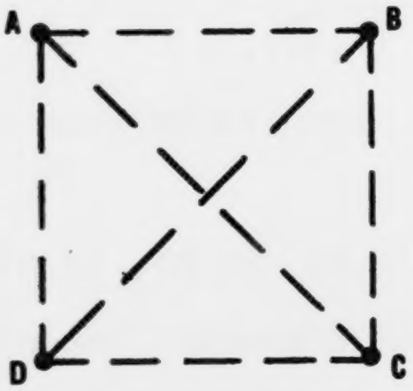


Figure 3.13

The diagram in Figure 3.13 can be viewed on its own merits as a set of four dots and a scheme for pairing these dots. This set of dots along with the scheme for pairing them two at a time, is still another model for our affine geometry. The dots in the model are the "points" of the geometry. The "lines" in this model are not the ordinary lines we draw with pencil and ruler. Here each "line" is simply a set of two dots with no other dots between the two. Certain "lines," such as the pairs of dots

{A,B} and {C,D}

which have no dot in common, are called "parallel lines." Notice that the two "lines"

{A,C} and {B,D}

are parallel according to this definition even though that may appear a bit queer, looking at the diagram. If we call the set of four dots "the plane π" we can then readily verify that this model satisfies Axioms 1, 2 and 3.

III. Let us look again at Figures 3.11, 3.12, and 3.13. You will observe that in each of these diagrams we deal with a basic set of four elements

$$\{A,B,C,D\}$$

and with the six subsets, each containing exactly two of the six elements:

$$\{A,B\}, \{A,C\}, \{A,D\}, \{B,C\}, \{B,D\}, \{C,D\}.$$

If we call any set of four elements "the plane π" and call each of the four elements a "point," and each of the six subsets, i.e. each pair of two elements, a "line," then we have still another model of a four point affine geometry. It does not matter what objects are used for this purpose. What does matter is that this scheme satisfies Axioms 1, 2 and 3 as can readily be verified.

A Nine Point Geometry

I. The corporation formed by our four enterprising businessmen is very successful. It expands by adding six more business enterprises and in doing so adds five new directors. In the course of this reorganization, it is decided to assign boards, consisting of three of the nine directors to manage the twelve business enterprises, a different set of three for each different enterprise. Once again, the assignments are to be made so that all nine directors will share equally in these management responsibilities.

Working out the details of the new organization turned out to be a bit tricky. Fortunately, one of the new directors had been a mathematics major at a university specializing in mathematical economics. He tackled the problem by viewing it as a nine point geometry. He represented the directors of the corporation by nine "points" labeled "A, B, C, D, E, F, G, H, I" and connected the "points" in sets of three by means of segments as indicated in Figure 3.14.

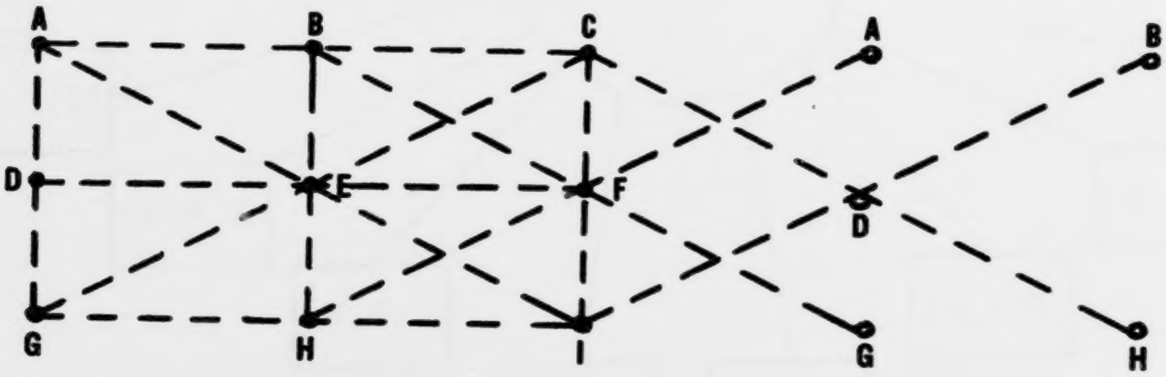


Figure 3.14

In this diagram the small circles do not represent new points. Each little circle represents the same point as the correspondingly labeled heavy dot. Placing these extra small circles alongside the actual array of nine dots is merely a convenient device for assigning the points in sets of three by connecting them with 12 segments as indicated. Each of the 12 segments now conveniently represents a board of directors assigned to one of the 12 business enterprises. The new corporate structure is displayed in Figure 3.15.

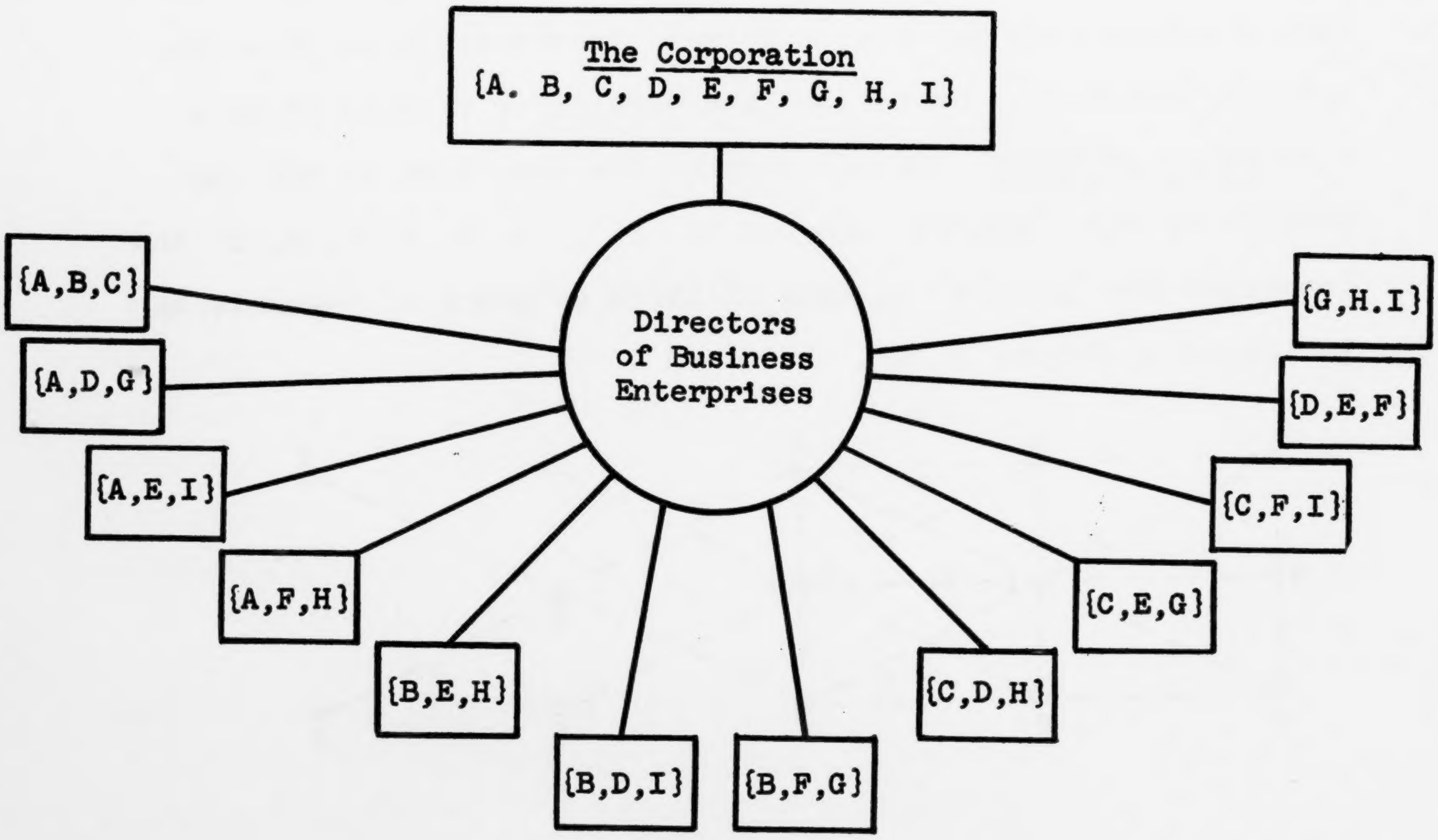

The Corporation
{A. B, C, D, E, F, G, H, I}
Directors of Business Enterprises
{A,B,C}
{A,D,G}
{A,E,I}
{A,F,H}
{B,E,H}
{B,D,I}
{B,F,G}
{C,D,H}
{C,E,G}
{C,F,I}
{D,E,F}
{G,H.I}

Figure 3.15

II. Now let us look again at Figures 3.14 and 3.15. In each diagram there is a basic set of 9 elements and certain specially selected subsets:

Plane π: {A,B,C,D,E,F,G,H,I}

Lines in π: {A,B,C} {B,E,H} {C,E,G}
{A,D,G} {B,D,I} {C,F,I}
{A,E,I} {B,F,G} {D,E,F}
{A,F,H} {C,D,H} {G,H,I}

Point: Any element in plane π.

Once again, it really does not matter what objects are chosen for the nine elements. What does matter is that this scheme is still another model for Axiom 1, 2, and 3 and therefore all the theorems that can be deduced from these axioms must hold in the model. This particular scheme is a "nine-point geometry."

Infinite Models

Models of this type will be described briefly in Section 3.14 and in greater detail in Chapter 6 (Coordinate Geometry). We mention these models at this point so that you will be aware of the fact that there are infinite models as well as finite ones.

You will recall that you used ordered pairs of integers as coordinates for lattice points in Chapter 7 of Course I (Lattice Points in the Plane). Any ordered pair (x,y) were $x \in Z$ and $y \in Z$ determined a unique lattice "point." Now there is no reason to confine ourselves to ZxZ, i.e. to integer values for x and y; we can also consider ordered pairs (x,y) where x and y are rational numbers. These ordered pairs of rational numbers can also be considered as coordinates for "points" in the more extensive set QxQ. This set contains all the lattice "points" of ZxZ as well as many other "in-between points."

Now it is possible to interpret plane π to be an infinite set of points such as QxQ, and to define certain (infinite) subsets of this plane π to be lines. This can be done in such a way as to satisfy Axioms 1, 2 and 3, thereby obtaining an infinite model for our axiomatic geometry. In Exercises 8 and 9 below you will have an opportunity to investigate infinite sets which obey some or all of our axioms. (The same technique can also be used to obtain interesting finite models. This is done by confining the coordinates x and y to finite number systems (clock arithmetics) such as Z_2 or Z_3 instead of infinite systems such as Z or Q.)

3.9 Exercises

1. Al, Bill, Carl and Don are tennis enthusiasts. The four boys organize themselves into a club called The Pioneers. The Pioneers plan to compete this season in a series of six tennis matches against doubles teams sponsored by other tennis clubs in town. The four boys are all excellent tennis players, so they agree to participate equally in the six tennis matches.
   - (a) For each of the six tennis matches, specify a doubles team which the Pioneers might assign to play that match. (Remember that each of the four boys must play equally often.)
   - (b) Show that this organization of the Pioneers into doubles teams can be interpreted as a model of our axiomatic geometry. Which model? What are the "points," "lines" and the "plane π" in this case?
   - (c) Express each of Axioms 1, 2 and 3 in the language of this model and verify that the axioms actually fit the model.
   - (d) Interpret each of the following terms in the tennis club model:

(1) parallel lines

(2) collinear points

(3) non-collinear points

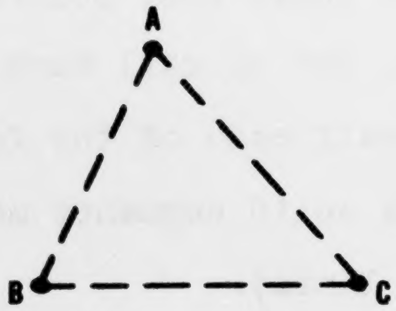
(4) concurrent lines

(e) Interpret Theorems 1, 2 and 3 in the language of this model. Why are Theorems 2 and 3 "trivial" in this case?

(f) Which of the theorems of axiomatic geometry could you use to prove that each of the Pioneers will play in at least two matches and will not play in at least two (other) matches.

2. Consider the following "three-point geometry" (see Figure below)

Plane π: {A,B,C}
Lines: {A,B}, {A,C}, {B,C}
Points: A, B, C



(a) Does this model satisfy the requirements of Axiom 1? Axiom 2? Axiom 3?

(b) Do there exist two (distinct) parallel lines in this model? Explain.

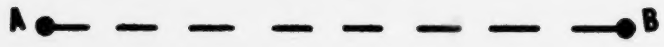
(c) Are the three points of this model collinear or are they non-collinear?

(d) Which of the following theorems is valid for this model?

(In each case try to explain why the theorem is valid or not valid by referring back to your answer to part (a) of this exercise.)

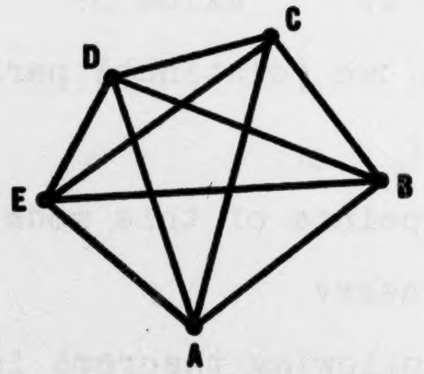
(1) Theorem 1
(2) Theorem 3
(3) Theorem 5
(4) Theorem 8
(5) Theorem 9
(6) Theorem 10

3. (a) Set up a geometry model using just two points A and B. In this model what is plane π? What are the lines? Which of our axioms are satisfied by this model?



*(b) Prove that any model which satisfies Axioms 1, 2 and 3 must contain at least four points.

4. In the figure below, let us call each vertex A, B, C, D, E a point and let us call each of the following pairs of vertices a line (the solid segments merely indicate which pairs of points are lines):
{A,B}, {A,C}, {A,D}, {A,E}, {B,C}, {B,D}, {B,E}, {C,D}, {C,E}, {D,E}.



By the plane π we mean the set $\{A,B,C,D,E\}$.

(a) Verify Axiom 1 (a).

(b) Verify Axiom 1 (b).

(c) Which of the following pairs of "lines" are parallel and which are not parallel?

(1) $\{A,B\}$ $\{B,C\}$

(2) $\{A,C\}$ $\{B,C\}$

(3) $\{A,C\}$ $\{B,D\}$

(4) $\{A,C\}$ $\{B,E\}$

(d) Is Axiom 2 satisfied?

(e) Is Axiom 3 satisfied? Explain.

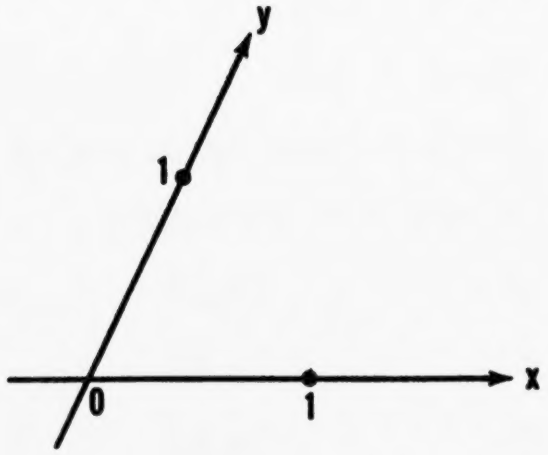
(f) For each point and each line not containing this point, how many lines are there containing the point and parallel to the line?

5. Theorem 13 asserts that there are at least four points in plane π, no three of which are collinear. Show that there need not be more than four. (Which model verifies this?)

6. Let the values of x and y be chosen from the number system $\{Z_2,+,\cdot\}$ where $Z_2 = \{0,1\}$. Define point to be any ordered pair (x,y) in $Z_2 x Z_2$; define the plane π to be $Z_2 x Z_2$, and define line to be the solution set of any equation of the form $ax + by = c$ where a, b and c are numbers in Z_2, and not both a and b are zeros.

(a) List all "points" in plane π.

(b) Plot these points on a graph using only the numbers in Z_2 as coordinates (See figure.)



(c) List all possible equations of the form $ax + by = c$ where a, b and c are in Z_2 and not both a and b are zeros. (Hint: There are six such equations. One of them is $1x + 0y = 1$. List the others.)

(d) For each of the six equations you listed in (c), determine its "line," i.e. the set of "points" (ordered pairs) in its solution set.

(e) Indicate these "lines" on your graph, connecting the points with dashed segments.

*7. Repeat each part of Exercise 6 using Z_3 instead of Z_2. There will be 9 points in this model.)

8. Let plane π consist of all ordered pairs of integers; i.e. $\pi = ZxZ$, and define a line to be the solution set in ZxZ of any equation of the form $ax + by = c$ where a, b, c are integers and a and b are not both zeros.

(a) Verify that this model satisfies Axiom 1(a). (Hint: you must find two equations of the form $ax + by = c$ with a and b not both zero, such that these two equations define two distinct "lines" i.e. the solution sets must not be the same. Try the two equations

$$1x + 0y = 0 \text{ and } 0x + 1y = 0.$$

What are the solution sets for these "lines"?)

(b) Verify Axiom 1 (b) for the "line" defined by each of the following:

(1) $x - y = 0$

(2) $x + y = 2$

(3) $2x - y = 0$

(4) $3x + 4y = 5$

(c) Verify Axiom 2 for each of the following pairs of points. (I.e., for each pair of points show that there is one and only one line containing both points.)

(1) $(0,0)$ and $(1,1)$

*(2) $(4,-1)$ and $(2,0)$

*(d) Set up a counter example to show that Axiom 3 is not satisfied in this model.

9. (a) In Exercise 8, if we define the plane $\underline{\pi}$ to be QxQ (instead of ZxZ), will your answers to parts (a) and (b) still be correct? Explain.

(b) Will your counter example for Exercise 8 (d) still be valid? Explain.

(c) Given the "line" m defined by $3x + 4y = 5$ and the "point" $E = (2,1)$ which is not contained in line m. Verify Axiom 3 for this case. (To do this you must find an equation in the form $ax + by = c$ where a and b are rational numbers not both zero, such that this equation is satisfied by the coordinates of E, but is not satisfied by the coordinates of any point in m. Then you must show that the line defined by this equation is unique, i.e. that any other equation which meets the requirements defines the same line.)

10. Suppose that a family is divided into committees such that:
    (1) Each committee has at least 2 members.
    (2) There are at least two committees and one committee has exactly 3 members.
    (3) Each committee has one member from each other committee.
    (4) Each two family members serve together on exactly one committee.
    (a) Using dots to represent individual members of the family and segments connecting these dots to represent committees, draw a model for these instructions.
    (b) Prove there must be at least four people in the family.
    (c) If we call each person a point and each committee a line, are there any parallel lines in this model? Why?

11. (a) Prove (Theorem 14): There are at least six lines in plane π.
    (b) Interpret this theorem in relation to the four point geometry model.

3.10 Equivalence Classes of Parallel Lines

According to Definition 1, two lines are parallel if they have no points in common, and each line is parallel to itself. The latter part of this definition asserts that

$$m \parallel m \text{ for every line } m.$$

You will recall that this can also be expressed by saying that

parallelism is a reflexive relation on the set of lines in π.

(See Course 1, Chapter 8, Sets and Relations)

Definition 1 also implies that

if $m \parallel n$ then $n \parallel m$,

which can also be expressed by saying that

parallelism is a symmetric relation on the set of lines in π.

This is easily proved as follows: if $m \parallel n$ then by Definition 1

either $m \cap n = \emptyset$ or $m = n$.

But both of these alternatives are symmetric, i.e. $m \cap n = \emptyset$ or $n = m$. So if $m \parallel n$, it follows that $n \parallel m$.

A third important property of parallelism is the following:

If $m \parallel n$ and $n \parallel \ell$ then $m \parallel \ell$

As you will recall, this property can also be expressed by saying that

parallelism is a transitive relation on the set of lines in π.

This is most readily proved by showing that it is impossible for parallelism not to be transitive. In other words if $m \parallel n$ and $n \parallel \ell$ could it be possible that $m \nparallel \ell$ (m not parallel to ℓ)?

This would mean that m and ℓ are distinct lines which have a point, A, in common. But then there would be two lines m and ℓ containing A and parallel to n. (See Figure 3.16.) This violates Axiom 3 which says that there can be only one line containing A parallel to n. Therefore it follows that m and ℓ cannot have a point in common or $m \parallel \ell$.

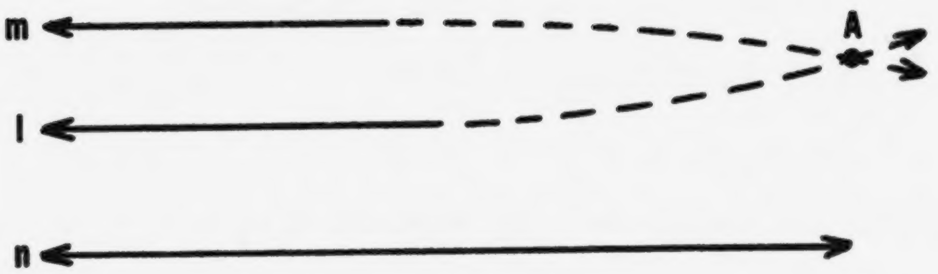


Figure 3.16

If $m \parallel n$ and $n \parallel \ell$, is it possible that $m \nparallel \ell$?

You will recall (see Course 1, Chapter 8, Sets and Relations) that a relation which is *reflexive*, *symmetric*, *and* *transitive* is also called an *equivalence relation*. We can therefore summarize what we have proved above in the following theorem:

Theorem 15. Parallelism is an equivalence relation on the set of all lines in plane π.

The most significant property of an equivalence relation in a set is that it always partitions the set into disjoint subsets. A relation R puts elements a and b in the same subset or equivalence class if and only if aRb. How does the equivalence relation "is parallel to" partition the set of lines in π into disjoint subsets?

To get a picture of the way the equivalence classes are determined by "$\parallel$," consider Figure 3.17.

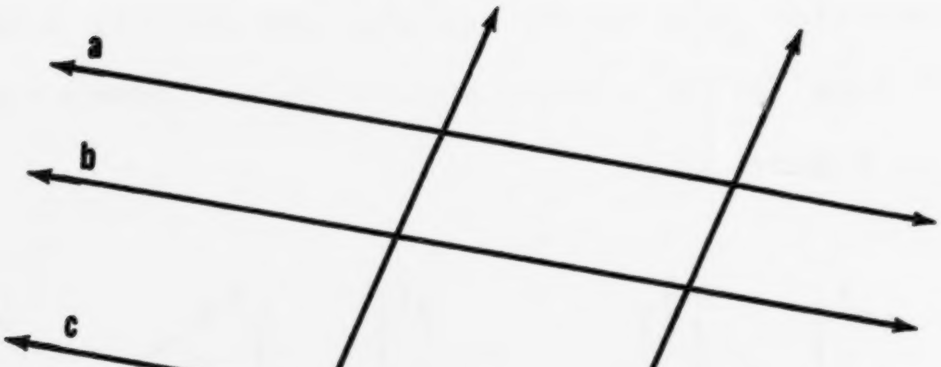


Figure 3.17

If lines which are related by "||" are put into the same class, the five lines pictured would be split into two classes, one containing a, b, and c, the other containing d and e. In a similar manner "||" partitions the set of all lines in π into disjoint equivalence classes; each class consists of all the lines in π that are parallel to a given line. We shall refer to "an equivalence class of parallel lines" here simply as "an equivalence class."

It is interesting to see what these equivalence classes are like in the various models we have constructed for our axioms. Consider the example, the four point model (Figure 3.18).

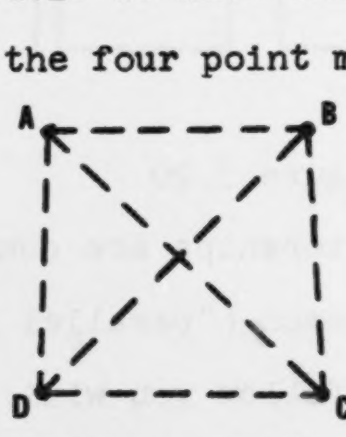


Figure 3.18

In this model the "plane" $\pi = \{A,B,C,D\}$ is partitioned by the parallelism relation into three equivalence classes each containing two "lines" of π. These equivalence classes can be pictured as in Figure 3.19.

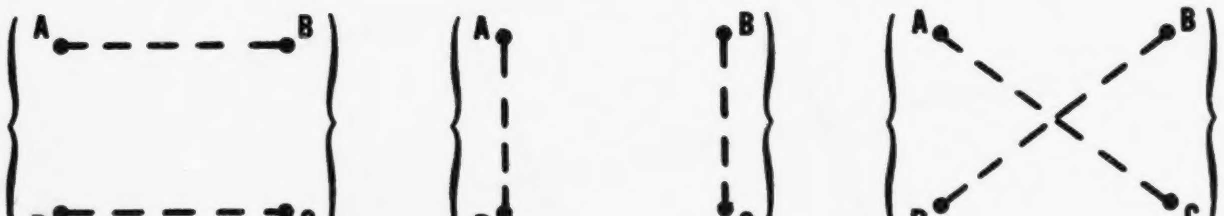

A
B
D
C
A
D
B
C
A
B
D
C

Figure 3.19

More precisely, each equivalence class is simply a set of subsets of π:

$\{\{A,B\}\ \ \{C,D\}\}\quad \{\{A,D\},\ \{B,C\}\}\quad \{\{A,C\},\ \{B,D\}\}$

If we re-interpret our "points," "lines," etc. in terms of our first business corporation model (see Section 3.8) the equivalence classes serve to partition the six boards of directors into three pairs as in Figure 3.20. (See also Figure 3.11.)

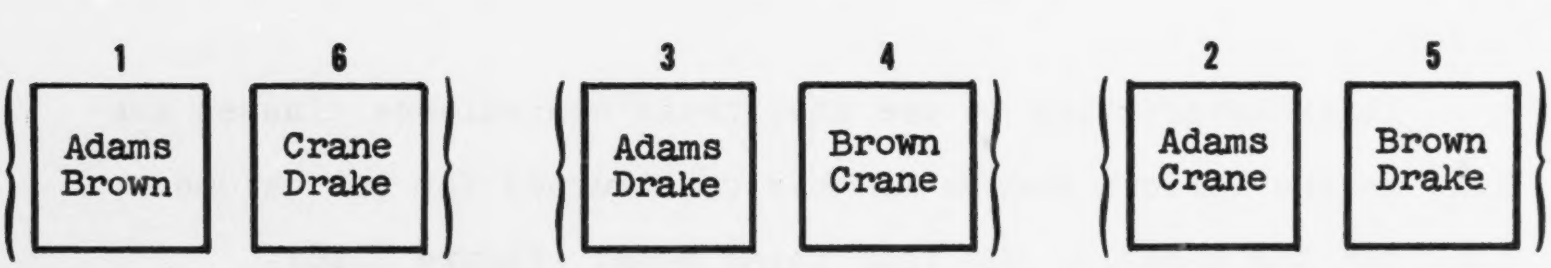

1
Adams
Brown
6
Crane
Drake
3
Adams
Drake
4
Brown
Crane
2
Adams
Crane
5
Brown
Drake

Figure 3.20

Within each pair, the directorships are completely distinct, i.e. they have no director in common ("parallel lines").

In the exercises that follow you will be asked to interpret the equivalence classes for other models.

3.11 Exercises

1. Which of the following are equivalence relations for the specified sets?
   - (a) "is the brother of" in the set of males.
   - (b) "is the same age as" in the set of living people.
   - (c) "is smaller than" in the set of students in your class.
   - (d) "has the same number of pages as" in the set of books.
   - (e) "is lighter than" in the set of students in your school.
   - (f) "is the line reflection of (in a fixed line)" in the set of points in a plane.
   - (g) "is perpendicular to" in the set of lines in a plane.
   - (h) "has a point in common with" in the set of lines in a plane.
   - (i) "is in the same grade as" in the set of students in your school.

   For each relation that actually is an equivalence relation, determine what kind of equivalence classes are formed.

2. Show that the relation "has the same author as" is an equivalence relation in the set of books in a bookstore. What kind of equivalence classes are determined by the relation?

3. Interpret the equivalence classes for the tennis club model (the Pioneers) of Exercise 1 in Section 3.9.

4. (a) Draw a diagram similar to Figure 3.19 showing all the equivalence classes for the nine-point geometry depicted in Figure 3.14.
   - (b) By drawing a diagram similar to Figure 3.20, interpret these equivalence classes to show how the set of twelve

business enterprises can be partitioned into subsets consisting of businesses whose directorships do not overlap.

5. Prove (Theorem 16): There are at least three distinct equivalence classes in plane π. (Hint: Use Theorem 12.)

6. Let D be an equivalence class which does not contain line m. If a second line n is parallel to m can D contain n? Prove your answer.

3.12 Parallel Projection

Because we will need the result of Exercise 5 in Section 3.11, it will now be proved. You may want to compare your proof with the proof given below.

Theorem 16. There are at least three equivalence classes in plane π.

Proof. Surely there is at least one point A in π. (In fact Theorem 13 asserts that there must be at least four points in π.) By Theorem 12 there are at least three (distinct) lines in π containing A. No two of these lines are parallel, since they are distinct and have point A in common. But in an equivalence class any two lines are parallel. Hence no two of these lines belong to the same equivalence class. Therefore the three lines belong to three (distinct) equivalence classes.

We shall now use the information that π has at least three different equivalence classes. Let m be any line in π and D any equivalence class not containing m. Let E be any point in π. From Axiom 3 we know that for every point E in π there is one and only one line, call it n, containing E which is in the equivalence class D (i.e. n is parallel to a line in D).

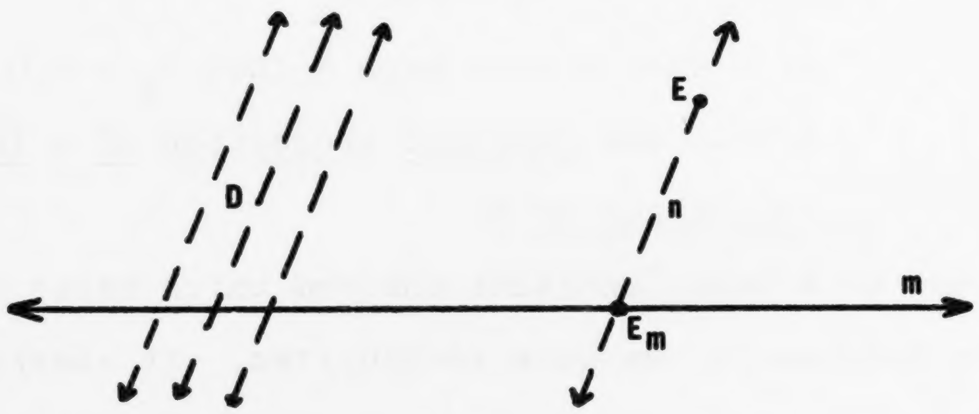


Figure 3.21

Moreover, n cannot be parallel to m. If it were, then m would be in the equivalence class of n which is D. We assumed that D was an equivalence class not containing m. If n and m are in different equivalence classes, n and m are distinct lines that have a common point E_m. So for every line m in π and equivalence class D not containing m, we have a mapping that sends each point E in the plane into a point E_m of line m. If we call this mapping "D_m," we have

$$E \xrightarrow{D_m} E_m$$

We can visualize the mapping D_m as projecting the point E from its position in plane π into a place in line m, by "moving" the point E "along" line n; and since n is parallel to all the lines in the equivalence class D, we call the mapping D_m a parallel projection.

Definition 4. Let m be any line in plane π, D any equivalence class in π that does not contain m, E any point in π, and n the line in D that contains E. The mapping

$$E \xrightarrow{D_m} E_m$$

of π into m that maps E into $E_m = n \cap m$, is called the parallel projection of π into m determined by D.

We now come to a very important theorem which makes use of almost all the information we have accumulated. It asserts that for any lines m and n in π, there is a parallel projection that maps n one-to-one onto m.

Theorem 17. In π, let m and n be any lines and let D be any equivalence class that contains neither m nor n. Then D_m is a parallel projection which maps n onto m. When the domain of D_m is restricted to n, D_m is one-to-one.

Proof. We must show two things:

1) D_m maps each point of n onto some point of m.
2) Under the "restricted" mapping D_m, each point of m is the image of exactly one point in n.

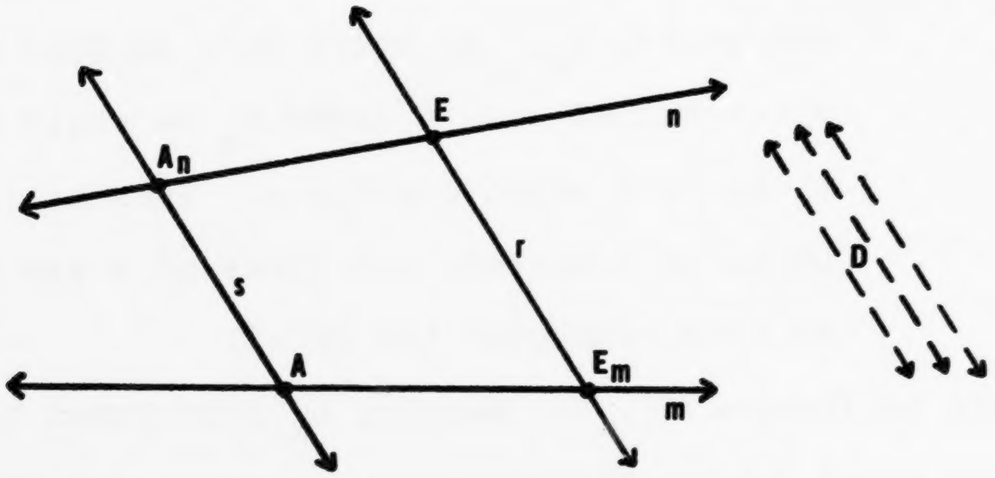


Figure 3.22

Let us first show that D_m maps each point of n onto some point of m. Let E be any point of n. (See Figure 3.22.) By Axiom 3 there is exactly one line in D, call it r, which contains E. We have selected equivalence class D so that m and n are not in D. Theorem 16 guarantees that such an equivalence class exists. It follows then that $r \cap m \neq \emptyset$ and $r \neq m$. Hence by Theorem 3, $r \cap m$ contains exactly one point, E_m. We have thus shown that D_m maps each point E of n onto some point, E_m, of m. To complete the proof we must show that when the domain of D_m is restricted to n, each point A of m is the image of exactly one point in n under this restricted mapping. Let s be a line in D which contains A. By Axiom 3 there is one and only one such line. As n is not in D, $s \cap n \neq \emptyset$ and $s \neq n$. It follows again by Theorem 3 that $s \cap n$ contains exactly one point, A_n. If there were another point in n which mapped onto A under D_m we would have two lines in D which contain A. This is impossible by Axiom 3 because the lines of D are parallel. We have completed the proof.

As proved in Theorem 17, the mapping D_m restricted to line n, establishes a one-to-one correspondence between the points in line n and the points in line m (see Figure 3.23).

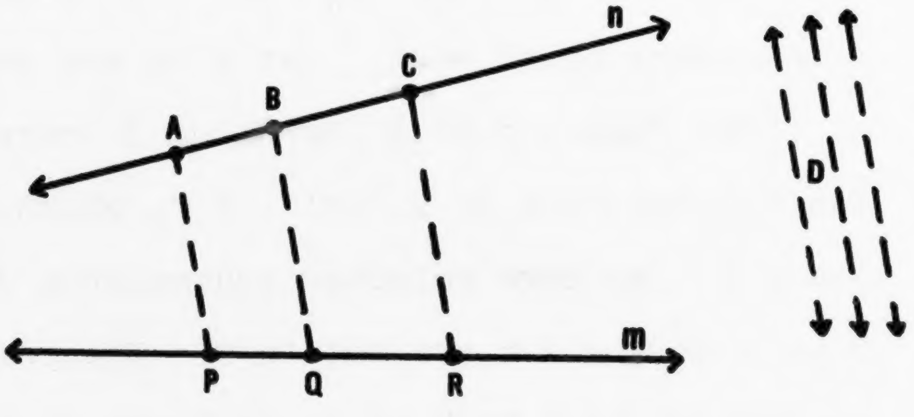


Figure 3.23

Each point, say A, B or C, in n has a unique image in m under D_m. Conversely, each point, say P, Q or R in m has a unique image in n, under D_n. The mapping D_n restricted to m, is the inverse of the mapping D_m restricted to n. Each of these mappings is called a parallel projection from one line onto the other line.

Definition 5. Let m and n be lines in plane π, and let D be any equivalence class in π which does not contain either m or n. The mapping D_m

restricted to n is called *a parallel projection from line n onto line m*. Its inverse mapping (namely D_n restricted to m) is called a parallel projection from line m onto line n.

It is an interesting logical consequence of Theorem 17 that all lines in π have the same number of points. For example, in a four point geometry, the plane π consists of four points. Each line in this plane π contains exactly two points. (How many points are there in each line of the nine-point geometry?) If even one line in π has infinitely many points, then every line n must have infinitely many points.

The notion of parallel projection constitutes the mathematical foundation on which to build coordinate systems for locating points in a plane. We can choose any two lines m and n in different equivalence classes and use these lines as "coordinate axes." (See Figure 3.24.)

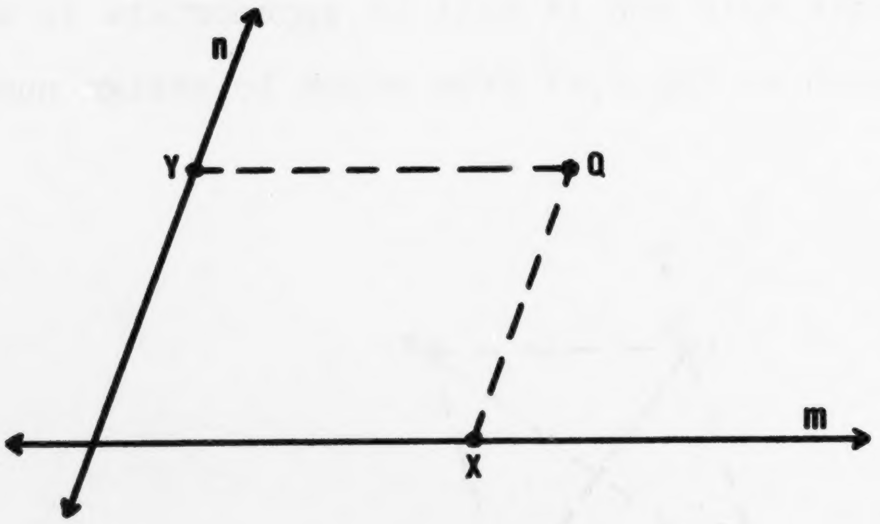


Figure 3.24

It can now be shown that for each point Q in the plane, there is a unique ordered pair of points (X,Y) where X is in m and Y is in N.

Point X is the image of Q under the parallel projection D_m of π into m determined by the equivalence class D that contains n. Point Y is the image of Q under the parallel projection D_n' of π into n determined by the equivalence class D' that contains m. The pair of points (X,Y) then serve as "coordinates" of point Q.

This idea of locating a point Q in plane π by referring to its "projections" on some chosen pair of "coordinate axes" is already familiar to you from your experience in drawing graphs. However you usually used a pair of numbers (x,y) rather than a pair of points (X,Y) for this purpose. To do this requires that there be some way of assigning a definite number to each point on every line in π (since any line in π could be chosen as one of the coordinate axes). The kind of numbers one may use for this purpose will depend on the geometric model being studied. For example, in a four-point geometry model, every line consists of exactly two points. Therefore there will be exactly two points on each coordinate axis and it will be appropriate to select a number system such as $\{Z_2,+,\cdot\}$ from which to assign numerical coordinates.

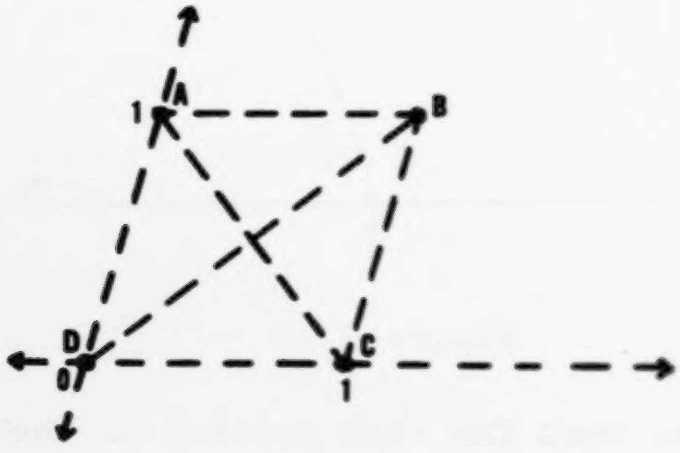


Figure 3.25

We may then assign the following coordinates (see Figure 3.25).

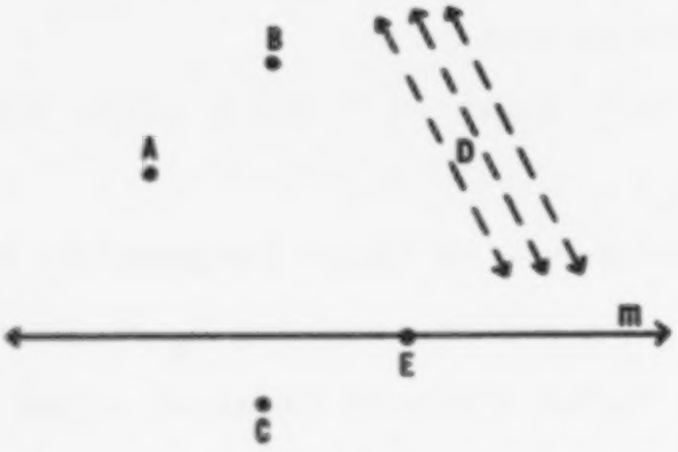
A(0,1)	B(1,1)	C(1,0)	D(0,0)

For more complicated geometric models more extensive number systems are needed. For infinite models infinite number systems such as the rational numbers or the real numbers are required. We shall return to this subject briefly in Section 3.14. In Chapter 6 we will discuss coordinates more extensively.

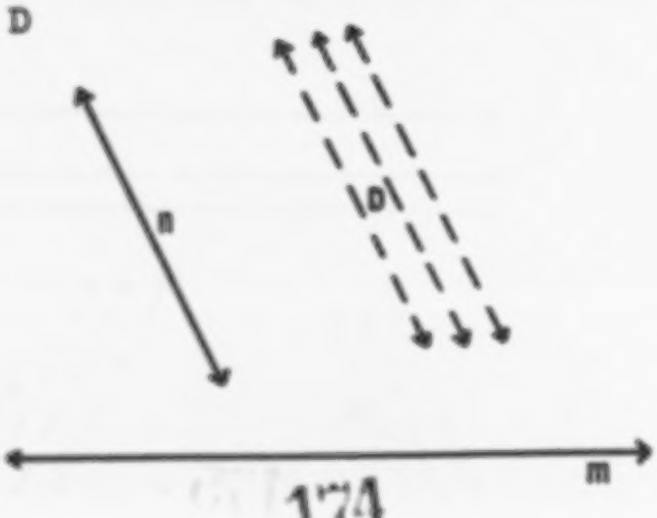
3.13 Exercises

(Copy each of the following diagrams in your notebook and use your notebook diagrams to answer the questions.)

1. Find the image of each of the points A, B, C and E under the parallel projection D_m.



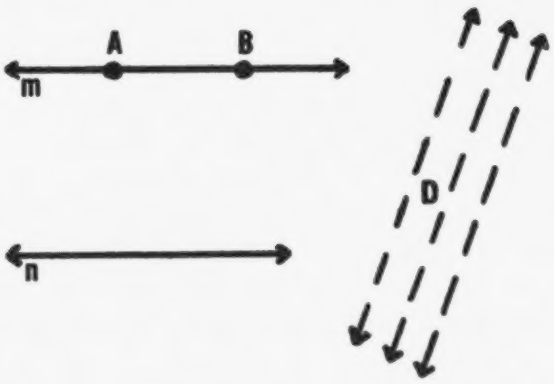
2. If D is an equivalence class containing line n and if m is a line not in D



(a) what is the image of each point of n under the parallel projection D_m?

(b) what is the image of each point of m under the parallel projection D_m?

3. Let $m \parallel n$ and let D be any equivalence class which does not contain either m or n.

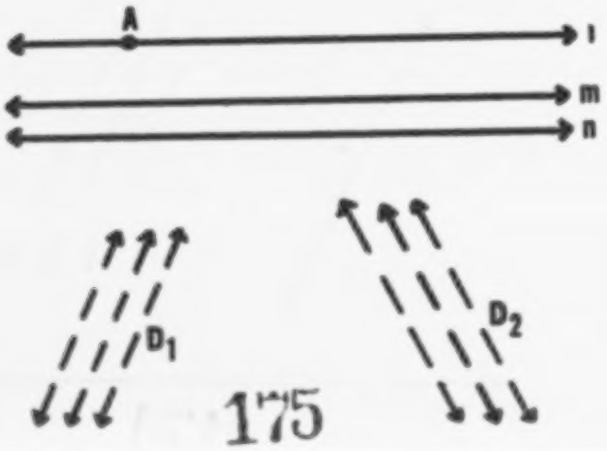


(a) If A and B are points in m, find their images under the parallel projection D_n. Call these image points C and D respectively.

(b) What are the images of C and D under the parallel projection D_m?

(c) What relationship is there between the mapping D_n restricted to m and the mapping D_m restricted to n?

4. Let ℓ, m, n be three distinct parallel lines and let D_1 and D_2 be two equivalence classes neither of which contains the lines ℓ, m or n. Let A be any point in line ℓ.



(a) Determine the image of A under each of the following parallel projections:

$(D_1)_m$, $(D_2)_m$, $(D_1)_n$, $(D_2)_n$

(b) Find the image of A under each of the following composite mappings:

(1) $(D_1)_m \circ (D_2)_n$ (2) $(D_2)_m \circ (D_1)_n$

(3) $(D_1)_n \circ (D_2)_m$ (4) $(D_2)_n \circ (D_1)_m$

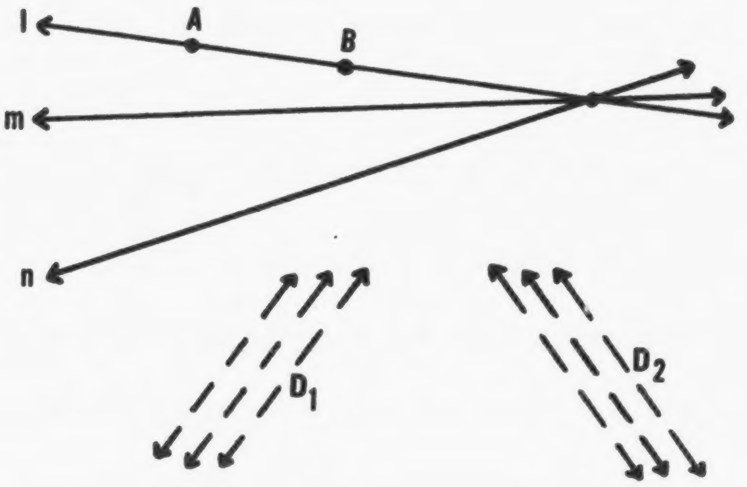
(c) Choose any point B in ℓ, other than point A, and repeat parts (a) and (b) of this exercise using point B. Try to formulate a general rule concerning the commuativity of parallel projections.

5. Copy the diagram in Exercise 4 on a large sheet of paper. Let f be the parallel projection from line ℓ to line m defined by restricting $(D_1)_m$ to line ℓ. Let g be the parallel projection from line m to line n defined by restricting $(D_2)_n$ to line m.

(a) Choose 2 different points A and B on line ℓ and determine the image of each of these points under the composite mapping g o f. Call these image points A' and B'. Draw segments $\overline{AA'}$ and $\overline{BB'}$.

(b) Repeat the experiment in (a) starting with at least two other pairs of points A_1, B_1 and A_2, B_2 on line ℓ. On the basis of your experiment does it appear that the composite mapping g o f is also a parallel projection from line ℓ to line n?

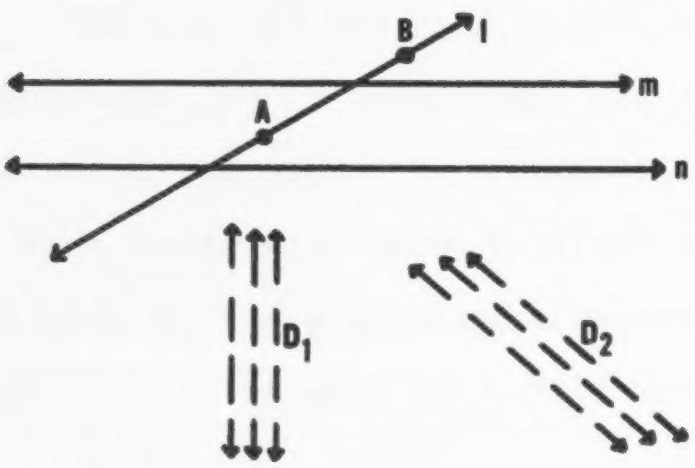
6. Let ℓ, m, n be three concurrent lines and let D_1 and D_2 be two equivalence classes not containing any of these lines. (See figure.)



Let f and g be parallel projections from ℓ to m and from m to n respectively as defined in Exercise 5.

Repeat parts (a) and (b) of Exercise 5 for these concurrent lines. Does the composite mapping g o f appear to be a parallel projection from ℓ to n in this case?

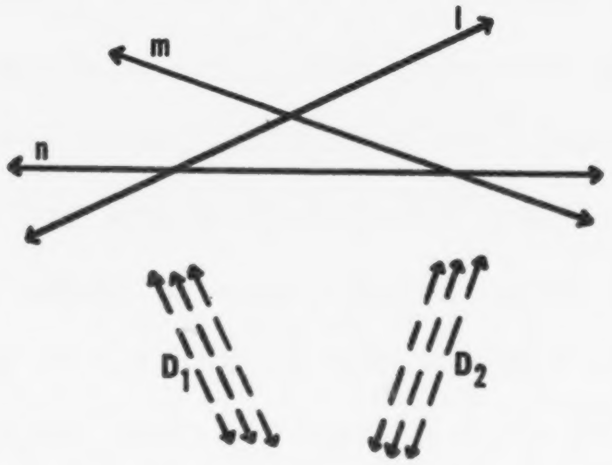
7. Suppose line ℓ intersects each of two parallel lines m and n and suppose D_1 and D_2 are two equivalence classes which do not contain any of the lines ℓ, m, n. (See figure.)



Let f and g be parallel projections from ℓ to m and from m to n, respectively, as defined in Exercise 5.

Repeat parts (a) and (b) of Exercise 5 for this situation. Does the composite mapping g o f appear to be a parallel projection from ℓ to n in this case?

8. Suppose ℓ, m, and n intersect in pairs as indicated, and suppose once again that D_1 and D_2 are distinct equivalence classes which do not contain any of the lines ℓ, m, n. (See figure.)



Let f and g be parallel projections from ℓ to m and from m to n respectively as defined in Exercise 5.

Repeat parts (a) and (b) of Exercise 5 for this situation. Does the composite mapping g o f appear to be a parallel projection from ℓ to n in this case?

3.14 Vectors -- An Intuitive Introduction

So far in this chapter we restricted our attention to some properties of the plane π which can be deduced logically from Axioms 1, 2 and 3 only. Because of this restriction we found it possible to admit a variety of models of our set of axioms, some of which may have been a bit unexpected.

In this section we are going to work with the "everyday" model that you would probably expect for the plane π. Our Axioms 1, 2 and 3 were selected so as to express some of the familiar properties of this everyday model, but by no means all of them. For example, in the everyday model the plane π actually contains infinitely many lines. In each line there are infinitely many points and "between" any two points there are always other points. In this section we shall assume some of these other properties, but such additional assumptions do not alter the fact that the "everyday" system is also a model for our original axioms.

Our specific reason for considering the "everyday" geometric model at this point is to use it in helping us understand the important concept of a vector. The notion of a vector is a remarkably useful one, not only for mathematicians but for physicists, engineers, economists and other scientists. For example physicists and engineers study forces and velocities as "vector quantities." Economists speak of "supply and demand vectors," "price vectors," etc. In this brief discussion, however, we shall confine oursleves to "geometric vectors." In Course III (in the chapter on Affine Geometry and Vector Spaces) we shall define a vector precisely.

To see how geometric vectors arise consider the following physical problem. The current in a river is flowing at a uniform rate. A rowboat, located originally at point A, is carried by the stream to point A' in one minute. A second rowboat, located originally at point B, is carried by the stream to point B' during the same minute of time. (See Figure 3.26.)

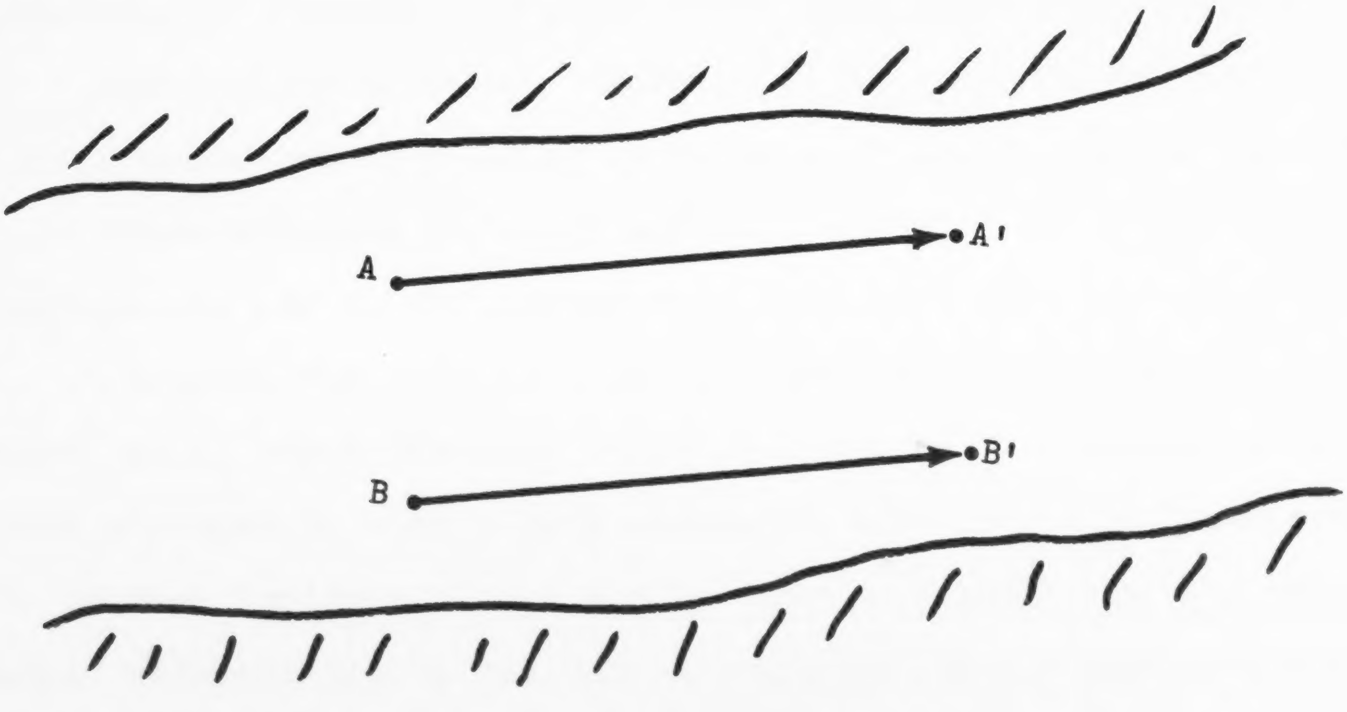


Figure 3.26

We may conveniently portray the motion of each boat by means of a "directed segment." This is simply a straight line segment joining the initial position of the boat to its final position. An arrow-head is placed at the terminal point of each segment to indicate the direction each boat has moved. It is convenient to use the symbols "$\overrightarrow{AA'}$" and "$\overrightarrow{BB'}$" to refer to these directed segments.

There is clearly a strong resemblance between these two directed segments. This resemblance is due to the fact that when the first boat moves from point A to point A' it is moving in the same direction and by the same amount as the second boat moves from point B to point B'. Mathematically, we may think of the river current as effecting a translation which maps point A onto point A', and also maps point B on to point B'. We can think of either of the directed segments $\overrightarrow{AA'}$ and $\overrightarrow{BB'}$ as "representing" this translation. Because $\overrightarrow{AA'}$ and $\overrightarrow{BB'}$ are "equally good" for this purpose we shall call these directed segments "equivalent."

Our use of the word "equivalent" is quite intentional. Whether a boat starts from point A, point B or any other point in the river, it is clear that the directed segments which represent the motion of each boat during let us say one minute, will all have the same length as well as the same direction. Let us imagine all possible directed segments drawn in an ordinary "everyday" plane π. The property, that a pair of segments shall "have the same length as well as the same direction" defines a bona fide equivalence relation in the set of all directed segments of π. To prove this, recall that you must show that the property in question is reflexive, symmetric and transitive. You should have no difficulty establishing each of these properties in the present situation. Equivalence of directed segments is therefore indeed an equivalence relation.

This equivalence relation partitions the set of all directed segments in plane π into equivalence classes. These equivalence classes are also called vectors. Since equivalent directed segments belong to the same equivalence class (i.e. the same vector) we also say that they represent the same vector. We express the idea that $\overrightarrow{AB}$ and $\overrightarrow{CD}$ represent the same vector by writing $\overrightarrow{AB} = \overrightarrow{CD}$.

For example in Figure 3.26 above we have $\overrightarrow{AA'} = \overrightarrow{BB'}$. Notice that this equation does not mean that $\overrightarrow{AA'}$ and $\overrightarrow{BB'}$ are the same directed segment, because they are not! It does mean that $\overrightarrow{AA'}$ and $\overrightarrow{BB'}$ represent the same vector: these directed segments belong to the same equivalence class.

For some further examples, suppose that A, B, C and D are points in plane π such that $\overrightarrow{AB} = \overrightarrow{CD}$. Figure 3.27 shows various possibilities for the directed segments.

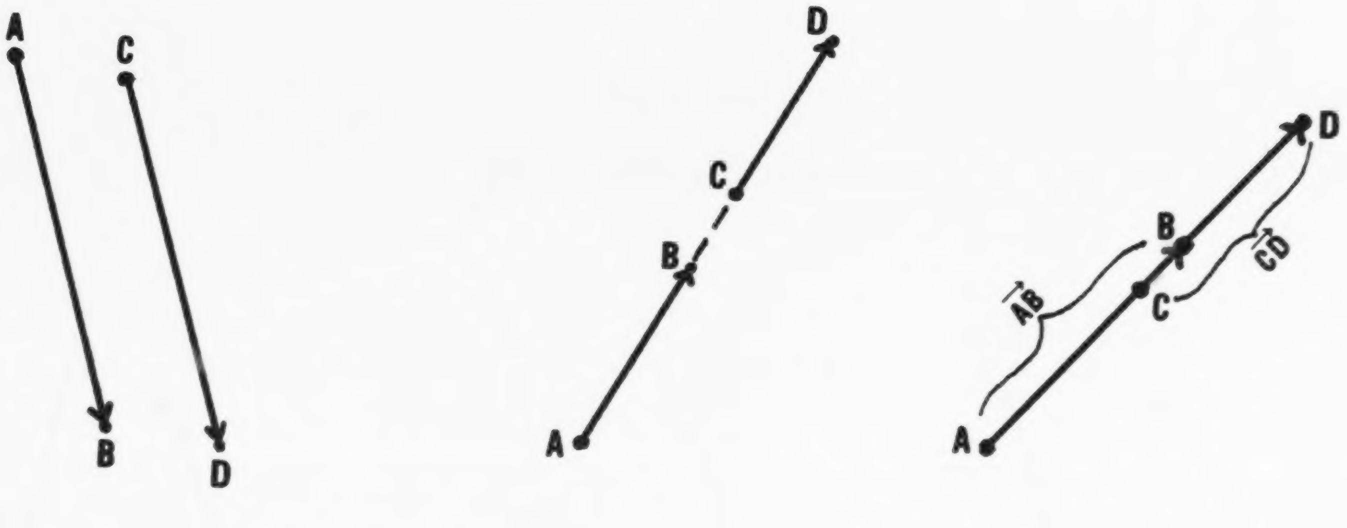
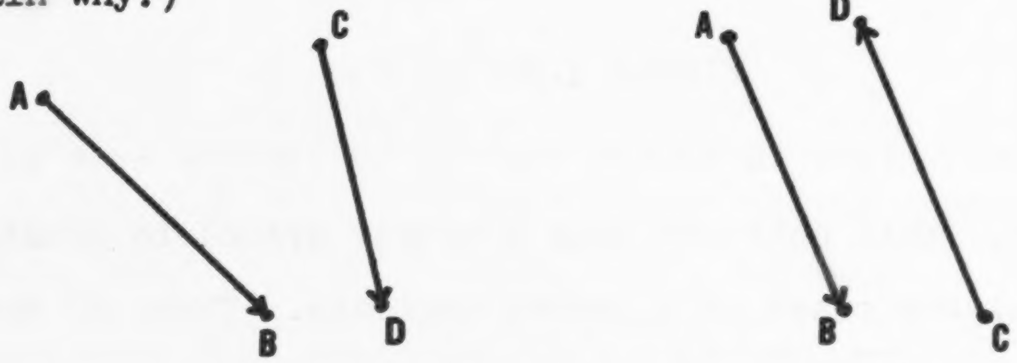


Figure 3.27

On the other hand, in Figure 3.28(a) and 3.28(b) we have $\overrightarrow{AB} \neq \overrightarrow{CD}$. (Explain why.)



(a) Figure 3.28 (b)

Similarly if A, B, C, D and E are such that

$$\overrightarrow{AB} = \overrightarrow{CD} = \overrightarrow{DE}$$

then these three directed segments might appear as in Figure 3.29

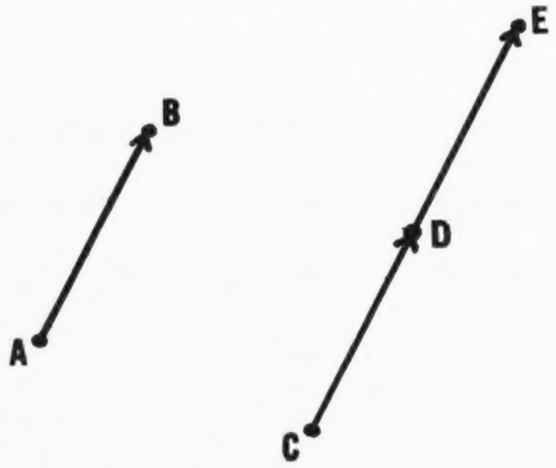


Figure 3.29

but *not* like *any* of these (in Figure 3.30)

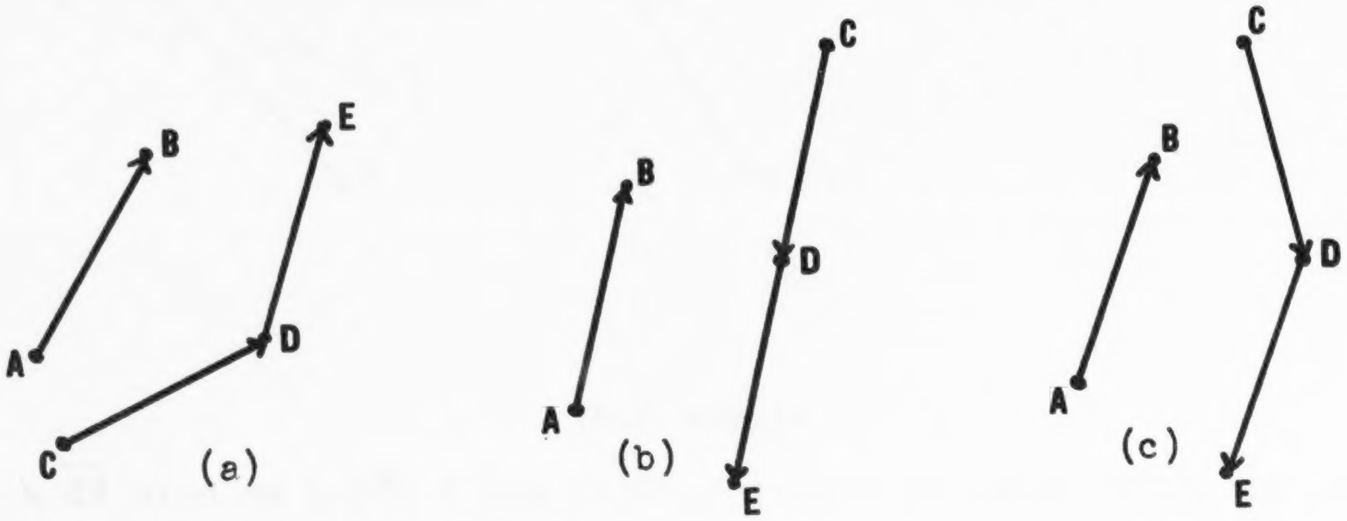


Figure 3.30

It is often convenient to denote vectors by symbols such as "$\vec{a}$," "$\vec{b}$," "$\vec{x}$," etc. This notation uses a single symbol to denote an entire equivalence class of directed segments. Thus, if the directed segments $\overrightarrow{AB}$, $\overrightarrow{CD}$, $\overrightarrow{EF}$, etc. each represent the same vector i.e. if $\overrightarrow{AB} = \overrightarrow{CE} = \overrightarrow{EF}$, etc., then this vector, let us call it "$\vec{a}$," corresponds to a translation which maps A onto B, C onto D, E onto F, etc. (See Figure 3.31)

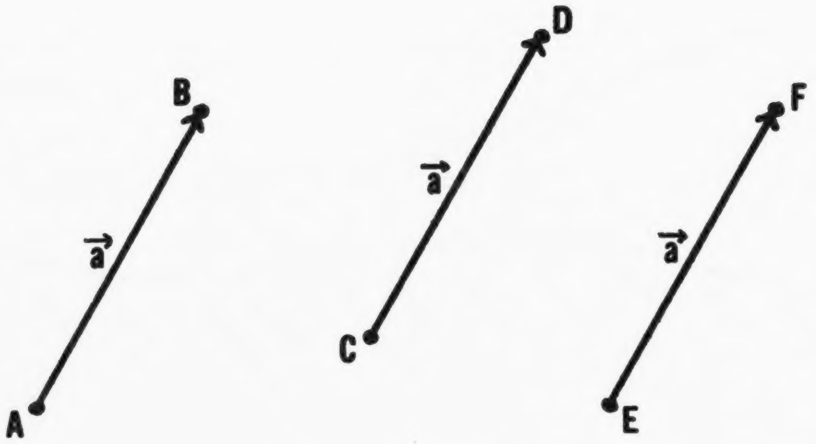


Figure 3.31

Observe that the symbol "$\vec{a}$" next to each of the directed segments, signifies that they all represent (i.e. belong to) the same vector $\vec{a}$. A particularly useful thing we can do is "add" vectors. How shall we define such "addition"?

We can take our cue from the idea that a vector corresponds to a translation which maps the plane π onto itself. To see this in a "practical" setting let us return to our illustration of a rowboat in a river flowing at a uniform rate. Temporarily, suppose there were no current flowing. The boat would of course remain motionless, unless someone in the boat started to row. If the occupant of the boat were to row at a uniform rate, the boat would move in the direction of rowing as long as there was no current. For example, after one minute the boat might move from point A to point B as in Figure 3.32.

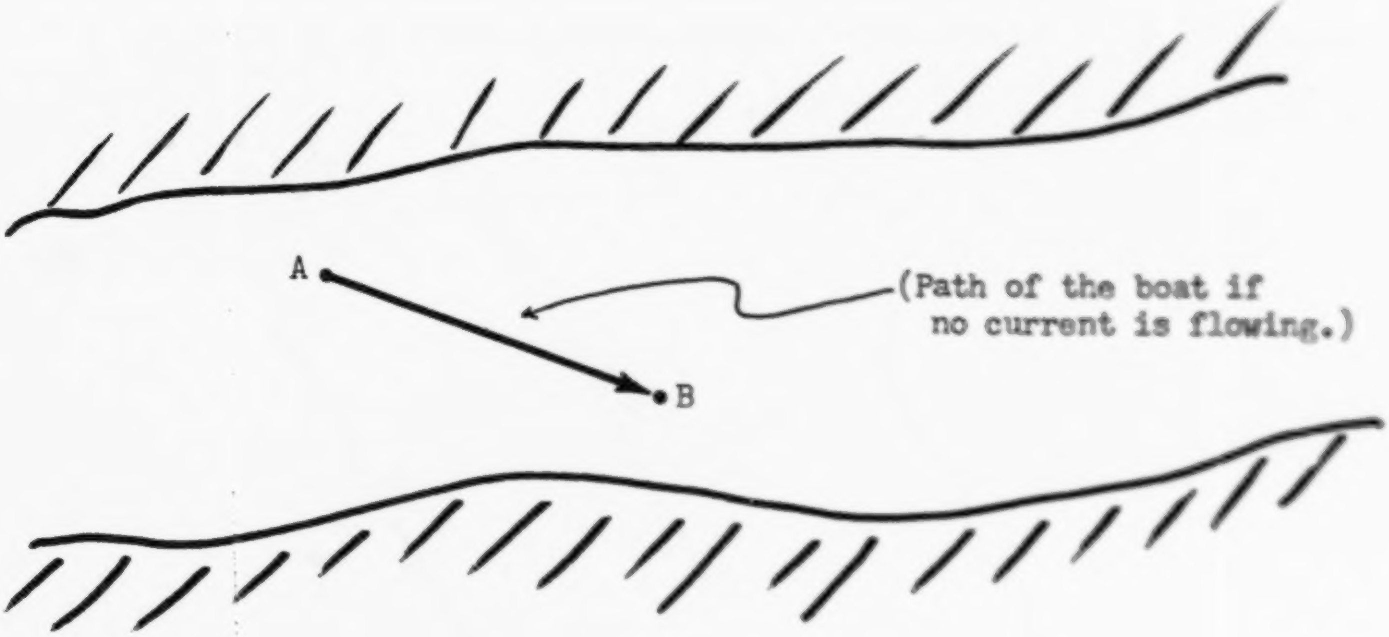

A
B
(Path of the boat if no current is flowing.)

Figure 3.32

Suppose now that the river is actually flowing at the uniform rate. Then, during this time, each point along the path of the boat is "translated" by the current to a new position. For example, point A is translated to A' and point B to B' (as Figure 3.33). The resulting ("resultant") path actually travelled by the boat is indicated in the following diagram (Figure 3.33).

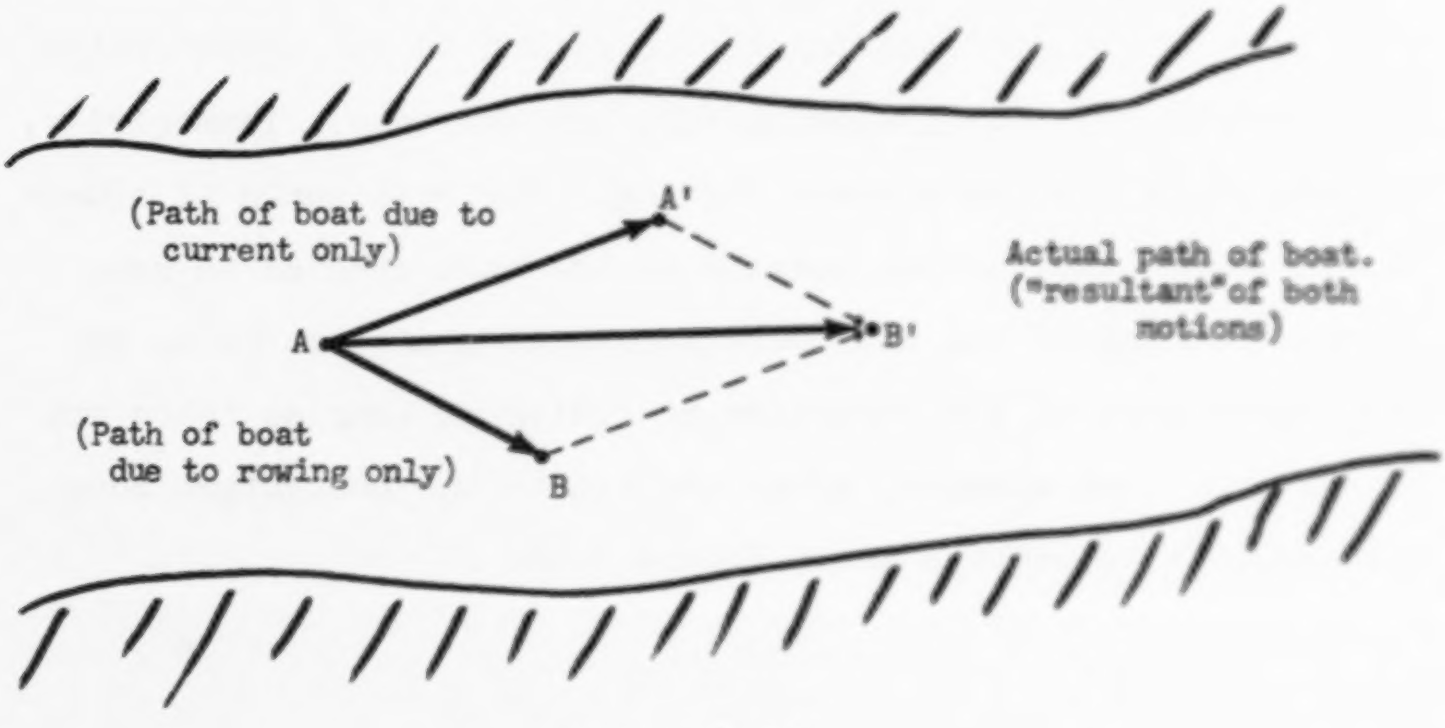

(Path of boat due to current only)
A'
Actual path of boat. ("resultant"of both motions)
A
B'
(Path of boat due to rowing only)
B

Figure 3.33

As we have previously indicated, the directed segments $\overrightarrow{AA'}$ and $\overrightarrow{BB'}$ are equivalent i.e. they represent the same vector. Let us call this vector $\vec{a}$. We write:

$$(1) \qquad \vec{a} = \overrightarrow{AA'} = \overrightarrow{BB'}$$

Similarly the directed segments $\overrightarrow{AB}$ and $\overrightarrow{A'B'}$ are also equivalent. Let us call the vector they represent $\vec{b}$:

$$(2) \qquad \vec{b} = \overrightarrow{AB} = \overrightarrow{A'B'}$$

The "resultant" directed segment $\overrightarrow{AB'}$ represents still another vector which we shall call $\vec{c}$. It is only natural that we agree to call this new vector, $\vec{c}$, the sum of vectors $\vec{a}$ and $\vec{b}$, and write:

$$(3) \qquad \vec{a} + \vec{b} = \vec{c}$$

As we have already noted in (1), the vector $\vec{a}$ can be represented by any directed segment in the equivalence class $\vec{a}$, and similarly, as in (2), the vector (equivalence class) $\vec{b}$ can be represented by any of its directed segments. We may therefore express the relationship (3) above in various alternative ways:

$$\overrightarrow{AA'} + \overrightarrow{AB} = \overrightarrow{AB'}$$

or

$$\overrightarrow{AA'} + \overrightarrow{A'B'} = \overrightarrow{AB'}$$

or

$$\overrightarrow{AB} + \overrightarrow{BB'} = \overrightarrow{AB'}$$

The first alternative here is usually described as the parallelogram rule for addition of vectors, because the directed segments $\overrightarrow{AA'}$ and $\overrightarrow{AB}$ form two adjacent sides of a parallelogram whose diagonal $\overrightarrow{AB'}$ represents their sum (see Figure 3.33). The second and third alternatives are usually referred to as the triangle rule for addition of vectors because for example $\overrightarrow{AA'}$ and $\overrightarrow{A'B'}$ form two sides of a triangle whose third side $\overrightarrow{AB'}$ represents their sum (see Figure 3.33).

Observe however that the sum

$$\vec{a} + \vec{b}$$

of a pair of vectors is defined even if these vectors are represented by directed segments which do not form a triangle. For example, in Figure 3.34 if $\overrightarrow{AB}$ represents vector $\vec{a}$ and if $\overrightarrow{CD}$ represents vector $\vec{b}$, then the sum $\vec{a} + \vec{b}$ is represented by the segment $\overrightarrow{EF}$ even though $\overrightarrow{AB}$, $\overrightarrow{CD}$ and $\overrightarrow{EF}$ do not form a triangle.

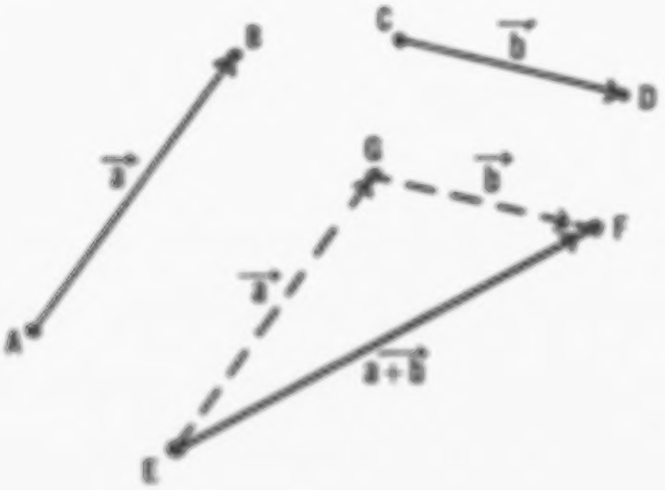


Figure 3.34

Notice however that the sum $\vec{a} + \vec{b}$ is most conveniently obtained by choosing a new pair of directed segments such as $\overrightarrow{EG}$ and $\overrightarrow{GF}$ which do form a triangle and which also represent vectors $\vec{a}$ and $\vec{b}$ respectively. Furthermore since

$$\overrightarrow{EG} + \overrightarrow{GF} = \overrightarrow{EF}$$

and $\qquad \overrightarrow{EG} = \overrightarrow{AB}, \quad \overrightarrow{GF} = \overrightarrow{CD}$

we may also write $\qquad \overrightarrow{AB} + \overrightarrow{CD} = \overrightarrow{EF}.$

This equation simply means that the vector represented by $\overrightarrow{EF}$ is the sum of the vectors represented by $\overrightarrow{AB}$ and $\overrightarrow{CD}$.

Figure 3.35 illustrates what happens if we reverse the order of addition of a pair of vectors.

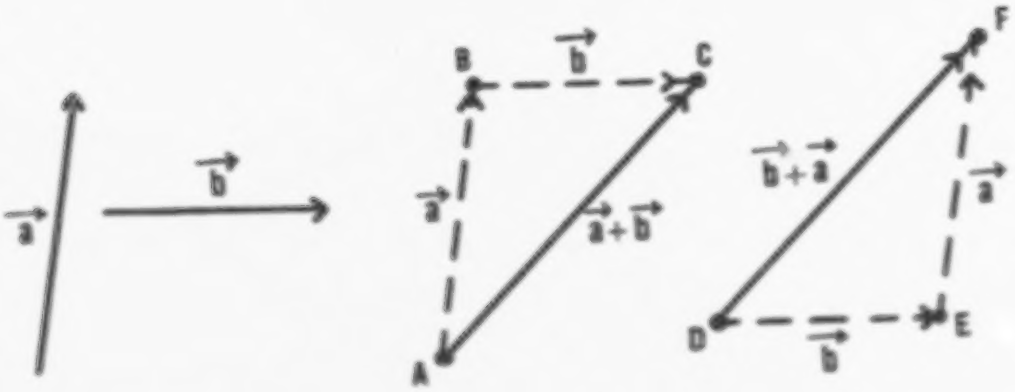

$\vec{a}$
$\vec{b}$
B
$\vec{b}$
C
$\vec{a}$
$\vec{a}+\vec{b}$
A
F
$\vec{b}+\vec{a}$
$\vec{a}$
D
$\vec{b}$
E

Figure 3.35

Notice that $\overrightarrow{AC} = \overrightarrow{DF}$. In fact we can imagine that triangle DEF is "moved" alongside triangle ABC as indicated in Figure 3.36.

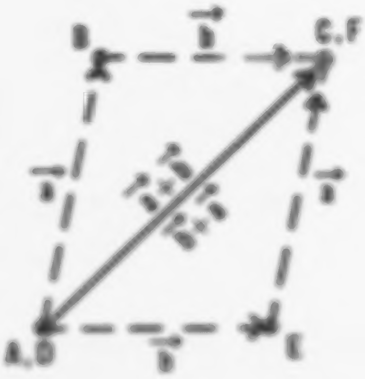

B
$\vec{b}$
C,F
$\vec{a}$
$\vec{a}+\vec{b}$
$\vec{b}+\vec{a}$
$\vec{a}$
A,D
$\vec{b}$
E

Figure 3.36

These diagrams illustrate the important fact that addition of vectors is commutative.

$$\vec{a} + \vec{b} = \vec{b} + \vec{a}$$

for all pairs of vectors $\vec{a}$ and $\vec{b}$. Looking at Figure 3.36 we see that the commutative law for addition of vectors is actually a consequence of the parallelogram law.

The triangle law can be extended so as to obtain a sum of any number of vectors. For example to add vectors $\vec{a}$, $\vec{b}$ and $\vec{c}$, in Figure 3.37 we use the triangle law to find $\vec{a} + \vec{b}$ and then use the triangle law again to find $(\vec{a} + \vec{b}) + \vec{c}$.

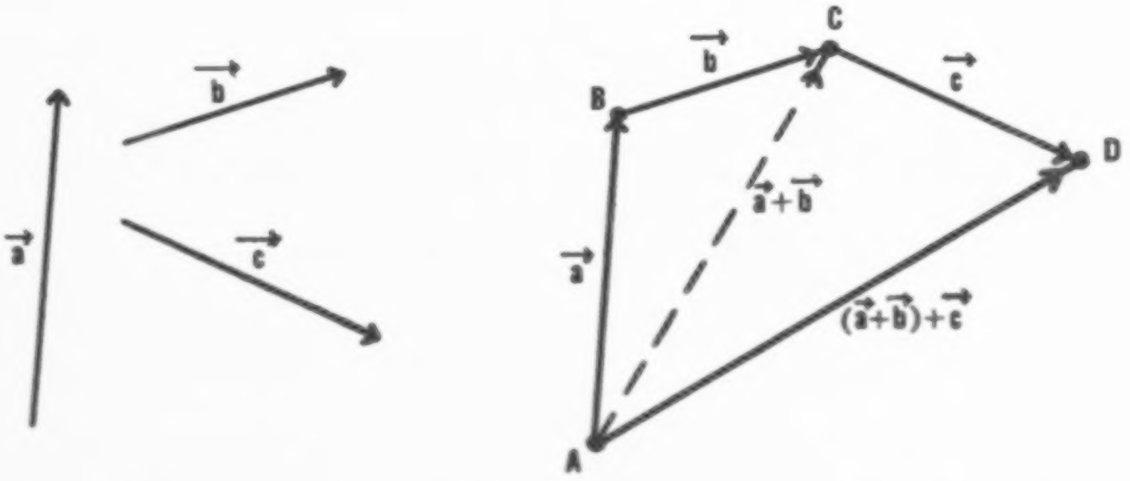


Figure 3.37

In Exercise 4 you will be asked to verify that the same sum is obtained by adding $\vec{a}$ to the sum $(\vec{b} + \vec{c})$. The fact that

$$(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$$

for all vectors $\vec{a}$, $\vec{b}$, $\vec{c}$ is called the associative law for addition of vectors.

Because of the appearance of Figure 3.37 this method of determining a sum of vectors is often called the vector polygon method.

In the exercises that follow you will be asked to discover other interesting properties of vectors.

3.15 Exercises

1. Suppose that the figure below is a parallelogram. How many distinct vectors are represented by:

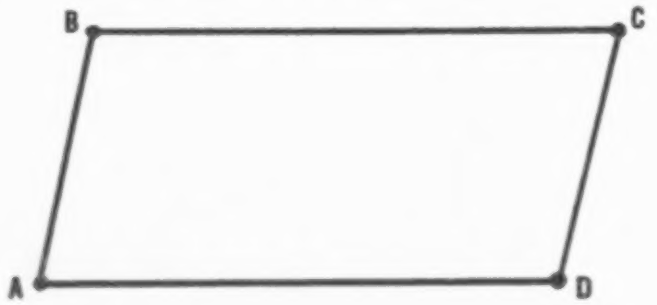
(a) $\overrightarrow{AB}$ and $\overrightarrow{DC}$

(b) $\overrightarrow{AB}$ and $\overrightarrow{CD}$

(c) $\overrightarrow{AB}$ and $\overrightarrow{BA}$

(d) $\overrightarrow{AB}$ and $\overrightarrow{AD}$

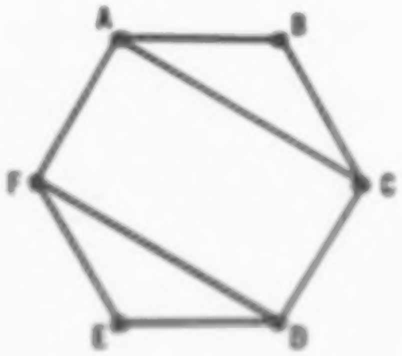
(e) $\overrightarrow{AD}$, $\overrightarrow{AC}$, $\overrightarrow{BC}$ and $\overrightarrow{CA}$.



2. Assume the figure below is a regular hexagon. This is a six sided polygon which possesses line symmetry about each of its diagonals. (See Course 1, Chapter 10, Segments, Angles and Isometries.)

   (a) How many distinct vectors are represented by $\overrightarrow{AB}$, $\overrightarrow{BC}$, $\overrightarrow{CA}$, $\overrightarrow{FE}$, $\overrightarrow{ED}$, $\overrightarrow{DF}$?

   (b) Which of these directed segments represent the same vector?



3. Draw suitable diagrams to find the following sums (by the triangle law):

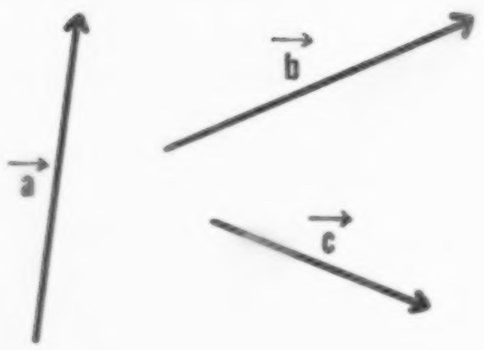
   (a) $\vec{a} + \vec{b}$

   (b) $\vec{b} + \vec{c}$

   (c) $\vec{a} + \vec{c}$

   (d) $\vec{b} + \vec{a}$

   (e) $\vec{c} + \vec{a}$



4. (a) For the vectors in the preceding figure draw diagrams to find each of the following sums:

$$(\vec{a} + \vec{b}) + \vec{c}$$
$$\vec{a} + (\vec{b} + \vec{c})$$

   (b) Compare the sums obtained in (a). What law is illustrated here?

   (c) Check your conclusion by using various other directed segments to represent vectors $\vec{a}$, $\vec{b}$ and $\vec{c}$.

5. For vectors $\vec{a}$, $\vec{b}$ and $\vec{c}$, as indicated in the adjoining figure, draw suitable diagrams to determine the following sums:

   (a) $\vec{a} + \vec{b}$ (b) $\vec{a} + \vec{c}$ (c) $\vec{b} + \vec{c}$

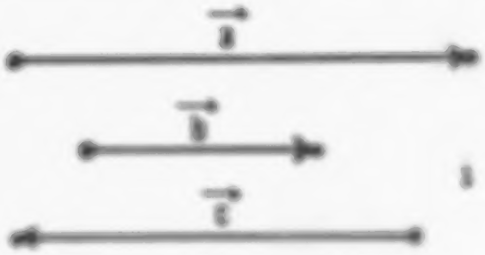


Figure for 5

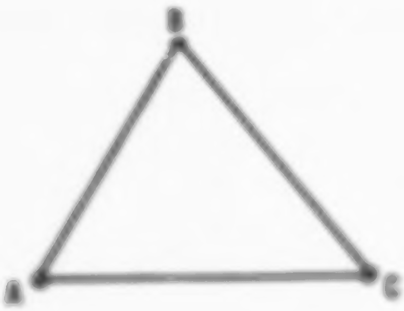


Figure for 6

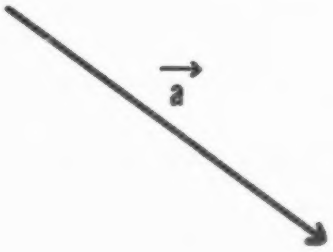
6. Using this figure draw diagrams to find the following sums:

(a)	$\overrightarrow{AB} + \overrightarrow{BC}$	(d)	$\overrightarrow{AB} + \overrightarrow{CB}$
(b)	$\overrightarrow{AB} + \overrightarrow{AC}$	(e)	$(\overrightarrow{AB} + \overrightarrow{BC}) + \overrightarrow{AC}$
(c)	$\overrightarrow{AB} + \overrightarrow{CA}$	(f)	$(\overrightarrow{AB} + \overrightarrow{BC}) + \overrightarrow{CA}$

Is there anything unusual about this last result? Explain.

7. For vector a represented in this figure draw diagrams to obtain:

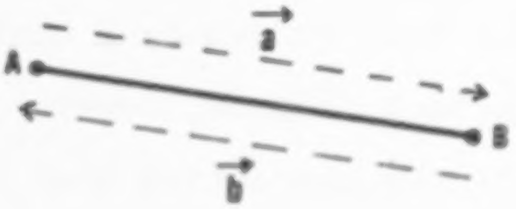
(a) $\vec{a} + \vec{a}$ (b) $(\vec{a} + \vec{a}) + \vec{a}$ (c) $(\vec{a} + \vec{a}) + (\vec{a} + \vec{a})$



Describe how each vector you obtain compares with vector $\vec{a}$. (Note: these new vectors are conveniently called $2\vec{a}$, $3\vec{a}$ and $4\vec{a}$.)

8. Let $\overrightarrow{AB}$ represent vector $\vec{a}$ and let $\overrightarrow{BA}$ represent vector $\vec{b}$ (in the adjoining figure).

(a) Draw a diagram to represent $\vec{a} + \vec{b}$.



Note: **In situations such as this we call the sum the zero vector and we denote it by "$\vec{0}$." The zero vector can be viewed as the equivalence class containing all "directed segments" of the form $\overrightarrow{AA}$, $\overrightarrow{BB}$, etc. (i.e. all directed segments $\overrightarrow{XY}$ were X = Y).**

(b) What is the sum $\vec{a} + \vec{0}$? $\vec{b} + \vec{0}$? $\vec{0} + \vec{a}$? $\vec{0} + \vec{b}$? $\vec{0} + \vec{0}$? State a general rule concerning addition of any vector to the zero vector.

9. By using equivalent directed segments or by reasoning from properties of translations, give an argument to show that if $\vec{a}$ is any vector, there is a unique (one and only one) vector $\vec{x}$ such that

$$\vec{a} + \vec{x} = \vec{0}$$

Note: the unique vector $\vec{x}$ which satisfies this equation is called the negative of vector $\vec{a}$ and is designated by $-\vec{a}$. The vector $-\vec{a}$ has the property

$$\vec{a} + (-\vec{a}) = (-\vec{a}) + \vec{a} = \vec{0}.$$

3.16 Summary

1. This chapter has dealt with axiomatic affine geometry, where a plane π is simply a set of points with certain interesting subsets called lines. The lines were assumed to have the properties mentioned in three axioms and from these properties we were able to deduce a number of other properties. It is important to note, however, that we were not able to deduce all the properties that we generally associate with lines and planes. In fact we studied a variety of models of affine geometry, in which the three axioms were satisfied, but in some of these models there were only four points, in other models there were exactly nine points in plane π and each line contained exactly three points;

still another model is the "everday" system of geometry in which the plane π contains infinitely many lines, each line contains infinitely many points, etc.

The three axioms used were

Axiom 1. (a) Plane π is a set of points, and it contains at least two lines.

(b) Each line in plane π is a set of points, containing at least two points.

Axiom 2. For every two points in plane π there is one and only one line in π containing them.

Axiom 3. For every line m and every point E in plane π there is one and only one line in π containing E and parallel to m.

Axioms 1 and 2 are called incidence axioms.

Parallel lines were defined as follows:

Lines r and s in π are parallel if and only if $r = s$ or $r \cap s = \emptyset$.

Using this definition we were able to prove that parallelism is an equivalence relation on the set of lines in π. This relation partitions the set of lines in π into equivalence classes, two lines being in the same equivalence class if and only if they are parallel.

The notion of an equivalence class of lines in π led to the following important consequences of the axioms:

(a) There are at least three equivalence classes in π.

(b) To every equivalence class D in π and line m in π but not in D there is a parallel projection, D_m, which maps all the points π onto m.

(c) For every two lines m and n in π there is a parallel projection that maps n onto m and is one-to-one. Coordinate systems for locating points in the plane π are based on these theorems concerning parallel projections.

If additional assumptions are added to the axioms for an affine plane, it will become possible to study the notion of a vector more precisely. We shall do this in Course III in the chapter on Affine Geometry and Vector Spaces. Meanwhile we have seen that we can base the notion of a vector on the idea of a directed segment. In fact a vector is an equivalence class of directed segments. It corresponds to a translation of the points of plane π. Addition of vectors corresponds to composition of translations. It is commutative, associative, and possesses an identity element (the zero vector $\vec{0}$) as well as an inverse ($-\vec{a}$) for each vector $\vec{a}$.

3.17 Miscellaneous Exercises

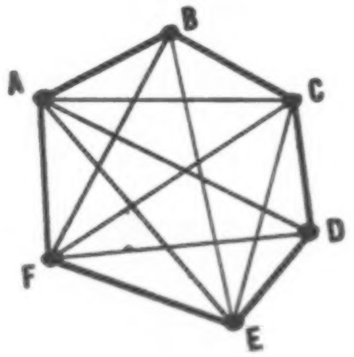
1. Prove that any "plane π" which obeys Axioms 1 and 2 must contain at least 3 non-collinear points and at least 3 non-concurrent lines.
2. Consider the following "six-point geometry":

Plane P. The set of 6 vertices:

$\{A, B, C, D, E, F\}$

Line. Any pair of distinct vertices.

Point. Any one of the 6 vertices.



(a) Indicate which of the Axioms 1, 2, 3 are true in this model and which are not true.

(b) Consider the line {A,B} and the point F not in this line. How many lines are there which contains F and are parallel to {A,B}? Name them.

(c) Name all lines that contain A and are parallel to the line {F,B}.

3. Prove that in any model which satisfies Axioms 1, 2, 3 there must be at least four lines no three of which are concurrent.

4. (a) Complete the following table for affine geometries:

	No. of points in each line	No. of lines containing each point	No. of points in plane π	No. of lines in plane π.
Four Point Geometry	2		4	
Nine Point Geometry	3		9	
	4			

(b) Try to formulate a general rule (see the next exercise).

*5. In an affine geometry prove that if one of the lines in plane P contains exactly k points then:

(a) every line contains exactly k points.

(b) each point is contained in exactly k + 1 lines.

(c) the plane π contains exactly k^2 points.

(d) the plane π contains exactly $k \cdot (k + 1)$ lines.

CHAPTER 4

FIELDS

4.1 What is a Field?

In Chapter 2 you saw that much of your knowledge of number systems can be expressed in the language of operational systems and groups. For instance, the set of integers under the operation of addition, $(Z,+)$, constitutes a group. The set of integers under the operation of multiplication, $(Z,\cdot)$, does not constitute a group, since only 1 and -1 have multiplicative inverses; but the non-zero rational numbers under the operation of multiplication, $(Q\setminus\{0\},\cdot)$ does constitute a group.

Such observations are helpful summaries of crucial properties in the various number systems, but they do not tell the whole story. Group theory only deals with properties of operational systems $(S,*)$ involving a set and a single operation. Most number systems with which you are familiar consist of a set S and two operations $+,\cdot$; the operations interacting via a distributive property, such as

$$a\cdot(b + c) = (a\cdot b) + (a\cdot c)$$

for all $\underline{a},\underline{b},\underline{c}$ in S.

In this chapter we will focus attention on a class of two-fold operational systems called fields. The study of groups brings insight and economy to the study of operational systems by developing properties common to a variety of specific systems. In the same way, the study of fields will develop properties common to many, but not all, two-fold operational systems.

4

Definition 1. A two-fold operational system $(F,+,\cdot)$ is called a field if and only if it satisfies the following axioms.

Axiom 1. For all a, b, c in F, $(a + b) + c = a + (b + c)$.

Axiom 2. There is an element 0 in F such that for all a in F, $a + 0 = a$.

Axiom 3. For each a in F there is an element -a in F such that $a + (-a) = 0$.

Axiom 4. For all a , b in F, $a + b = b + a$.

Axiom 5. For all a, b, c in F, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$.

Axiom 6. There is an element 1 in F $(1 \neq 0)$ such that for all a in F, $a\cdot 1 = a$.

Axiom 7. For each a in F $(a \neq 0)$, there is an element a^{-1} in F such that $a\cdot a^{-1} = 1$.

Axiom 8. For all a, b in F, $a\cdot b = b\cdot a$.

Axiom 9. For all a, b, c in F, $a\cdot(b + c) = (a\cdot b) + (a\cdot c)$.

There are three questions suggested immediately by this definition. First, why was this particular collection of axioms chosen? Second, are there any familiar two-fold operational systems that obey the field axioms? Third, what is the significance of choosing "+" and "·" to name the operations in a field and "0" and "1" to name the respective identity elements?

If you look closely at Axioms 1 through 4, you see that they guarantee that the system $(F,+)$ is a commutative group with identity element 0. Furthermore, unless 0 causes some unforeseen difficulties in multiplication, it appears that the system $(F\setminus\{0\},\cdot)$ is a commutative group with identity element 1. Thus in a sense, a field is two groups which interact via a distributive property.

The most familiar examples of fields are the system (Q,+,·) of rational numbers under addition and multiplication and several finite number systems, such as $(Z_3,+,\cdot)$ and $(Z_5,+,\cdot)$.

These examples indicate why the symbols "+," "·," "0," and "1" are used instead of some more general symbols like "$*_1$," "$*_2$," "e_{*_1}," and "e_{*_2}." But as you know, the "+" in (Z,+) has quite a different meaning than the "+" in $(Z_3,+)$. Thus, although for convenience "a + b" is often read "a plus b" and "a·b" as "a times b," it is important to keep in mind that there are fields in which "+" and "·" represent operations bearing little resemblance to addition or multiplication of rational numbers. Similarly "0" and "1" might represent objects quite different from rational numbers.

4.2 Exercises

1. In (Q,+,·) find the standard name for each of the following:
   (a) the additive inverse of
      (1) $\frac{2}{3}$
      (2) $\frac{3}{-4}$
      (3) $\frac{-7}{-8}$
      (4) $-\frac{1}{2}$
      (5) $\frac{231 - 11}{-3}$
      (6) $\frac{-3}{8} + \frac{2}{-5}$
      (7) $\frac{\frac{7}{-3}}{\frac{-5}{12}}$
      (8) 1
      (9) 0
   (b) the multiplicative inverse of each number in (a).
2. Compute in (Q,+,·):
   (a) $\frac{2}{3}\cdot(\frac{5}{8} + \frac{3}{4})$

(b) $\frac{2}{3} + (\frac{5}{8} \cdot \frac{3}{4})$

(c) $(\frac{2}{3} \cdot \frac{5}{8}) + (\frac{2}{3} \cdot \frac{3}{4})$

(d) $(\frac{2}{3} + \frac{5}{8}) \cdot (\frac{2}{3} + \frac{3}{4})$

(e) $(-\frac{4}{5} \cdot \frac{5}{6}) + \frac{7}{-12}$

(f) $(-\frac{4}{5} \cdot \frac{7}{-12}) + (\frac{5}{6} \cdot \frac{7}{-12})$

(g) $(-\frac{4}{5} + \frac{5}{6}) \cdot \frac{7}{-12}$

(h) $(-\frac{4}{5} + \frac{7}{-12}) \cdot (\frac{5}{6} + \frac{7}{-12})$

3. In $(Z_6, +, \cdot)$ compute

   (a) $3 \cdot (2 + (-4))$

   (b) $(3 \cdot 2) + (3 \cdot (-4))$

   (c) $3 + (2 \cdot (-4))$

   (d) $(2 + 3) \cdot (-4 + 3)$

4. In $(Z_6, +, \cdot)$ find the standard name for each of the following:

   (a) the additive inverse of

      (1) 0
      (2) 1
      (3) 2
      (4) 3
      (5) 4
      (6) 5

   (b) the multiplicative inverse of each number in (a).

5. In $(Z_7, +, \cdot)$ find the standard name for:

   (a) -3
   (b) -5
   (c) -0
   (d) 3^{-1}
   (e) 5^{-1}
   (f) 0^{-1}
   (g) $(-4 + 6)^{-1}$
   (h) $2 + (3 \cdot 5)$
   (i) $(2 + 3) \cdot (2 + 5)$

6. Determine whether or not each of the following two-fold operational systems is a field. If the system is not a field,

   (1) state each property that does not hold, and

   (2) give an example in which the property fails to hold.

      (a) $(W, +, \cdot)$

      (b) $(Z, +, \cdot)$

      (c) $(Q^{+}, +, \cdot)$ (See Chapter 2.)

      (d) $(Q^{\pm}, +, \cdot)$ (See Chapter 2.)

(e) $(Z_3,+,\cdot)$ (i) $(Z_8,+,\cdot)$

(f) $(Z_4,+,\cdot)$ (j) $(Z_9,+,\cdot)$

(g) $(Z_7,+,\cdot)$ (k) $(Z_{10},+,\cdot)$

(h) $(Z_{12},+,\cdot)$

*7. In which of the above two-fold operational systems is there an element _x_ such that $x^2 = 2$?

*8. In which of the above two-fold operational systems are there non-zero elements _a_ and _b_ such that $a \cdot b = 0$? In such systems, find as many of these elements as you can. Also, are any of the systems in which you find such elements fields?

*9. Show that in any system $(Z_n,+,\cdot)$, if $n = p \cdot q$ where _p_ and _q_ are integers (not = 1), there are elements _a_ and _b_ such that $a \cdot b = 0$.

**10. The operational system $(\{a,b,c,d,\},+,\cdot)$ has operations defined by the following tables:

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

Is this operational system a field? Why or why not?

4.3 Getting Some Field Theorems Painlessly

In any field $(F,+,\cdot)$, the additive structure $(F,+)$ is a commutative group with identity element 0. Therefore, any theorem proven in Chapter 2 for groups is automatically a theorem for $(F,+)$ and thus for $(F,+,\cdot)$.

For instance, in a group $(S,*)$, for each a in S, $(a^I)^I = a$. Translating this theorem into the language of $(F,+)$ yields Theorem 1.

Theorem 1. For all $a \in F$, $-(-a) = a$.

This is a familiar theorem in $(Q,+,\cdot)$. For a more interesting illustration and check, consider $-(-2)$ in $(Z_7,+,\cdot)$:

$$-(-2) = -(5) = 2$$

Another theorem of Group Theory states that for all a,b in S, $(a * b)^I = b^I * a^I$. This leads to Theorem 2 for fields. (Note: In this chapter it is understood that all operations are in $(F,+,\cdot)$ unless otherwise specified).

Theorem 2. For all a,b in F,

$$-(a + b) = (-b) + (-a).$$

Question. Why can we conclude also that

$$-(a + b) = (-a) + (-b)?$$

The third automatic consequence of the group properties in $(F,+)$ is a theorem about solvability of equations.

Theorem 3. For all a,b in F, the equation $x + a = b$ has a unique solution $x = b + (-a)$.

In the language of groups, the justifying theorem states that every equation $x * a = b$ has a unique solution $x = b * a^I$. In the case of a particular field, $(Z_7,+,\cdot)$, Theorem 3 implies that $x + 6 = 2$ has a unique solution $x = 2 + (-6) = 2 + 1 = 3$.

One of the most useful properties of any group is cancellation: For all a,b,c in S, if $a * b = a * c$, then $b = c$. This leads to an important theorem in $(F,+,\cdot)$.

Theorem 4. (cancellation) For all a,b,c in F, if $a + b = a + c$, then $b = c$.

Question. Which axiom allows us to deduce a right cancellation property now for "+" in $(F,+,\cdot)$?

4.4 Trouble with 0.

Although this chapter was advertised as a study of certain two-fold operational systems, there has been a conspicuous absence of results concerning the second field operation "$\cdot$" or results which relate addition and multiplication. You might well ask why multiplicative counterparts of the group theorems were not presented for $(F\setminus\{0\},\cdot)$. Isn't this system a group? The troublemaker in this situation is that single exception lurking inside the set brackets, the additive identity element 0.

In $(F\setminus\{0\},\cdot)$ multiplication is associative; it has an identity element, 1, and each element has an inverse. The only question is whether $(F\setminus\{0\},\cdot)$ is an operational system. If a and b are elements of $F\setminus\{0\}$, then we know that $a\cdot b \in F$. But could $a\cdot b = 0$? The answer is "no," but the proof is not trivial; it requires knowledge of the strange behavior of the additive identity under the operation of multiplication. As you might expect, the distributive property makes its grand entrance at this point.

Theorem 5. For all a in F, $a\cdot 0 = 0\cdot a = 0$.

Proof. 1. Since 0 is the additive identity element, $0 + 0 = 0$ and $(a\cdot 0) + 0 = a\cdot 0$.

2. Also $a\cdot 0 = a\cdot(0 + 0) = a\cdot 0 + a\cdot 0$.

3. By SPE, $a\cdot 0 + a\cdot 0 = a\cdot 0 + 0$.

4. Then Theorem 4 (cancellation) implies $a\cdot 0 = 0$.

5. Since multiplication is commutative, $a\cdot 0 = 0\cdot a$, and thus $0\cdot a = 0$.

Theorem 5 shows clearly why, in any field, 0 has no multiplicative inverse. There can be no element a in F such that $0\cdot a = 1$, because $0\cdot a = 0$ for all a in F and $0 \neq 1$.

Next, Theorem 6 is a converse of Theorem 5; it states if a product is 0, then one of the factors must be 0.

Theorem 6. For all a, b in F, if $a\cdot b = 0$, then $a = 0$ or $b = 0$.

Proof. 1. If $a\cdot b = 0$ and $a \neq 0$, then a has multiplicative inverse $\underline{a}^{-1}$ and $a^{-1}\cdot(a\cdot b) = a^{-1}\cdot 0 = 0$.

2. also $a^{-1}(a\cdot b) = (a^{-1}\cdot a)b = 1\cdot b = b$

3. Thus we conclude that $b = 0$. (SPE)

4. If $a\cdot b = 0$ and $b \neq 0$, then right multiplication by b^{-1} leads similarly to the conclusion $a = 0$.

Since $a\cdot b = 0$ if and only if $a = 0$ or $b = 0$, we are now justified in claiming that $(F\backslash\{0\},\cdot)$ is a group. Theorems 7 through 9 are the multiplicative counterparts of Theorems 1 through 3; proofs rest on the group theorems of Chapter 2.

Theorem 7. For all a in $F\backslash\{0\}$, $(a^{-1})^{-1} = a$.

Theorem 8. For all a,b in $F\backslash\{0\}$, $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$.

Theorem 9. For all a,b in $F\backslash\{0\}$ the equation $x\cdot a = b$ has a unique solution $x = b\cdot a^{-1}$.

The following examples interpret these theorems, which apply to all fields, in specific situations.

Example 1. In $(Z_7,+,\cdot)$, $3^{-1} = 5$ and $5^{-1} = 3$, since $3 \cdot 5 = 1$. Thus $(3^{-1})^{-1} = (5)^{-1} = 3$.

Example 2. In $(Q,+,\cdot)$, $(\frac{2}{3} \cdot \frac{5}{8})^{-1} = (\frac{10}{24})^{-1} = \frac{24}{10}$, but

$$(\tfrac{5}{8})^{-1} \cdot (\tfrac{2}{3})^{-1} = \tfrac{8}{5} \cdot \tfrac{3}{2} = \tfrac{24}{10} \text{ also.}$$

Example 3. In $(Z_7,+,\cdot)$ the equation $x \cdot 3 = 2$ has unique solution $x = 2 \cdot 3^{-1} = 2 \cdot 5 = 3$.

The following exercises explore several other applications of field theorems to specific situations. In each, be sure to check the definition of "+" and "$\cdot$" in the field being studied.

4.5 Exercises

1. Find the standard name for each of the following in $(Z_{11},+,\cdot)$:
   - (a) $-(3 + 7)$
   - (b) $-(-3 + (-7))$
   - (c) $-(-(-(8)))$
   - (d) 4^{-1}
   - (e) $((4^{-1})^{-1})^{-1}$
   - (f) $(4 \cdot 9^{-1})^{-1}$
2. State the group theorems (using $(S,*)$ and a^I notation) which justify
   (a) Theorem 7 (b) Theorem 8 (c) Theorem 9.
3. Prove: In $(F,\cdot)$, if $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$.
   (Hint: As in Theorem 6, $a \neq 0$; try a similar proof.)
4. Find the standard name for each of the following in $(Q,+,\cdot)$:
   - (a) $(-3) \cdot 7$
   - (b) $-(3 \cdot 7)$
   - (c) $3 \cdot (-7)$
   - (d) $(\frac{-5}{8}) \cdot (\frac{-2}{8})$
   - (e) $\frac{5}{8} \cdot \frac{2}{5}$
   - (f) $(-\frac{2}{3}) \cdot (-\frac{5}{6})$
5. Prove $a^2 \neq 0$ in $(F \setminus \{0\},\cdot)$ $[a^2 = a \cdot a]$

6. Compute in $(Z_7,+,\cdot)$:

(a) 1^2	(d) 4^2
(b) 2^2	(e) 5^2
(c) 3^2	(f) 6^2

7. Compute 4^2 in $(Z_8,+,\cdot)$.

8. Prove: For any a in F, if $a + b = a$, then $b = 0$.

9. Prove: For all a,b,c in F, $(b + c)\cdot a = b\cdot a + c\cdot a$.

*10. Prove: If $n = p\cdot q$ (when p,q are integers different from 1) then $(Z_n,+,\cdot)$ is not a field.
(Hint: Consider Theorem 6 and the result of Exercise 9 in Section 4.2).

4.6 Subtraction and Division in Fields

As you have noticed already, much of the theory for fields is suggested by observations in particular fields, often $(Q,+,\cdot)$. In the rational number system you found that $a - b = a + (-b)$. $(Q,+)$ is a group; and it is possible to introduce a similar subtraction in any group, $(F,+)$ in particular.

Definition 2. For all a,b in F, $a - b = a + (-b)$.
To see that this definition is reasonable in fields other than $(Q,+,\cdot)$, study these examples drawn from $(Z_7,+,\cdot)$.

Example 1. $3 - 1 = 3 + (-1)$
$= 3 + 6$
$= 2$

Example 2. $4 - 6 = 4 + (-6)$

Many of the properties of subtraction in $(Q,+,\cdot)$ carry over into the theory of fields.

Theorem 10. For all a,b,c in F:

(a) $a - a = 0$

(b) $a - 0 = a$

(c) $0 - a = -a$

(d) $a - b = a - c$ implies $b = c$

*(e) $a - b = c$ if and only if $a = c + b$.

Proof. Exercises.

There are many properties that could be listed, such as $a - (b - c) = (a - b) + c$. See if you can discover some of these and prove them. You will find some in the exercises that follow this section.

The definition of subtraction is fairly simple, but to work with this operation effectively, two more theorems are necessary.

Theorem 11. For all a,b in F:

(a) $-(a\cdot b) = (-a)\cdot b$

(b) $-(a\cdot b) = a\cdot(-b)$

(c) $a\cdot b = (-a)\cdot(-b)$

Proof. Since this theorem involves the behavior of additive inverses under multiplication, the proof of part (a) uses the distributive property. Parts (b) and (c) follow easily from (a), and those proofs are left as exercises.

(1) $-(a\cdot b) + (a\cdot b) = 0$ and

$(-a + a)\cdot b = 0\cdot b = 0.$

(2) By distributivity, $(-a + a)\cdot b =$

$(-a)\cdot b + (a\cdot b).$

(3) Therefore, using SPE

$-(a\cdot b) + (a\cdot b) = (-a)\cdot b + (a\cdot b)$.

(4) Then right cancellation implies that

$-(a\cdot b) = (-a)\cdot b$.

Theorem 12. For all a,b,c in F, $a\cdot(b - c) = a\cdot b - a\cdot c$.

Proof. Exercises.

It might surprise you, but Theorem 12 (and Theorem 11 on which it depends) is necessary to justify simplifications like $7x - 5x = 2x$ or to solve equations like $x^2 - 2x = 0$.

Example 3. $7x - 5x = x\cdot 7 - x\cdot 5$

$= x(7 - 5)$

Example 4. $x^2 - 2x = 0$ implies

$x\cdot x - x\cdot 2 = 0$ which implies

$x(x - 2) = 0$.

By Theorems 5 and 6, the product $x(x - 2)$ can equal zero if and only if at least one of the factors is zero; in other words, if $x = 0$ or if $x = 2$.

Just as subtraction can be defined in the additive structure of any field, a kind of generalized division can be introduced in terms of multiplication.

Definition 3. For all a,b in F $(b \neq 0)$,

$a \div b = a\cdot b^{-1}$.

As you probably expect, there are theorems about division analogous to those for subtraction.

Theorem 13. For all a,b,c in $F\setminus\{0\}$:

(a) $a \div a = 1$

(b) $a + 1 = a$

(c) $1 + a = a^{-1}$

(d) $a + b = a + c$ implies $b = c$

(e) $a + b = c$ if and only if $a = c \cdot b$.

Proof. Exercises.

4.7 Exercises.

1. Find standard names for each of the following in $(Q,+,\cdot)$:

(a) $\frac{11}{15} - \frac{2}{5}$ (d) $\frac{2}{3} + \frac{14}{6}$

(b) $-\frac{7}{5} - \frac{-2}{10}$ (e) $\frac{-3}{8} + \frac{7}{-9}$

(c) $-(\frac{3}{8} - \frac{2}{3})$ (f) $11 \cdot (\frac{-5}{22})$

2. Find standard names for each of the following in $(Z_7,+,\cdot)$:

(a) $(-3)(5)$ (c) $(-3)(-5)$ (e) $5 + 3$

(b) $-(-3)(5)$ (d) $-(-3)(-5)$ (f) $3 + 5$

3. Simplify the following expressions in $(Q,+,\cdot)$:

(a) $\frac{2}{3}x + \frac{7}{6}x$ (c) $(8x + \frac{1}{3}x) - \frac{5}{3}x$

(b) $\frac{2}{3}x - \frac{7}{6}x$ (d) $14 - (-8x - 7x)$

4. Find the solution set of the following open sentences in $(Q,+,\cdot)$. (Hint: See Examples 3 and 4 of Section 4.6.)

(a) $8x + \frac{1}{3}x = 7$ (d) $\frac{4}{3}x = x^2$

(b) $3x^2 - 2x = 0$ (e) $(x + 3)(x - \frac{1}{2}) = 0$

(c) $\frac{7}{8}x - \frac{1}{2}x^2 = 0$ (f) $(2x - \frac{1}{3})(\frac{3}{5}x + \frac{1}{2}) = 0$

5. Prove Theorem 10. (Hint: Part (a) is given as an example here.

The trick is to change subtraction expressions to equivalent addition expressions.)

Proof. $a - a = a + (-a)$ Definition 2 "-"

$= 0$ Definition of inverse

6. Prove Theorem 13. (Hint: Use a trick similar to that in Exercise 5)
7. Prove Theorem 12.

*4.8 Fractions in Fields

In the rational number system the notation "$\frac{1}{a}$" is commonly used to indicate the multiplicative inverse of a. Similarly, the notation "$\frac{a}{b}$" is used instead of "$a \div b$." This idea is generalizable to all fields as follows.

Definition 4. For all a,b in F ($b \neq 0$),

$$a \div b = a \cdot b^{-1} = \frac{a}{b}.$$

The division theorems can be translated into the language of fractions. Although this will then look very much like $(Q,+,\cdot)$, some oddities result when the symbolism is interpreted in finite fields. The following results are provable by application of Definition 4 and some algebraic manipulation. No proofs are given, but the exercises of Section 4.9 illustrate several of the properties and the techniques used in proofs.

Theorem 14. For all a,b,c,d in F ($b \neq 0$, $d \neq 0$):

(a) $\frac{a}{b} = \frac{c}{d}$ if and only if $a \cdot d = b \cdot c$.

(b) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

(c) $(\frac{d}{b})^{-1} = \frac{b}{d}$

(d) $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}$

Theorem 15. For all a,b in F ($b \neq 0$):

(a) $\frac{-a}{b} = \frac{a}{-b}$

(b) $-(\frac{-a}{b}) = \frac{a}{b}$

(c) $\frac{-a}{-b} = \frac{a}{b}$

(d) $-(\frac{a}{b}) = \frac{-a}{b}$.

*4.9 Exercises

1. Find the standard name for each of the following in $(Z_7, +, \cdot)$ by direct computation:

   (a) $\frac{3}{2}$ (ans. $\frac{3}{2} = 3 \cdot 2^{-1} = 3 \cdot 4 = 5$ or $\frac{3}{2} = 3 \div 2 = 5$ since $3 = 5 \cdot 2$)

   (b) $\frac{4}{5}$

   (c) $-\frac{4}{5}$

   (d) $\frac{-4}{5}$

   (e) $\frac{2}{3}$

   (f) $\frac{-2}{-3}$

2. Again in $(Z_7, +, \cdot)$, find the standard name for each of the following by direct computation:

   (a) $\frac{5}{6}$

   (b) $\frac{3}{5}$

   (c) $5 \cdot 5$

   (d) $6 \cdot 3$

   (e) $\frac{5 \cdot 3}{6 \cdot 5}$

   (f) $\frac{5}{6} \cdot \frac{3}{5}$

   Now look back at Theorems 14(a) and 14(b) !

3. Prove $\frac{d}{b} \cdot \frac{b}{d} = 1$ in every field $(F, +, \cdot)$.

   (Hint: Write $\frac{d}{b}$ as $d \cdot b^{-1}$ and $\frac{b}{d}$ as $b \cdot d^{-1}$ and simplify.)

4. Using Exercise 2 to save some work, compute in $(Z_7, +, \cdot)$:

   (a) $\frac{5}{6} + \frac{3}{5}$

   (b) $\frac{5 \cdot 5 + 3 \cdot 6}{6 \cdot 5}$

5. Using a = 5 and b = 2, check each part of Theorem 15 in Z_7.

by direct computation. (For example: $\frac{-5}{2} = (-5)\cdot 2^{-1} = 2\cdot 4 = 1$

and: $\frac{5}{-2} = 5\cdot(-2)^{-1} = 5\cdot(5)^{-1}$

$= 5\cdot 3 = 1.$)

6. Prove: For all a,b in F, $-(\frac{-a}{b}) = \frac{a}{b}$ $(b \neq 0)$. (Hint: $\frac{-a}{b} = (-a)\cdot b^{-1}$ and use Theorem 11.)
7. Prove: For all a,b in F, $-(\frac{a}{b}) = \frac{-a}{b}$.

4.10 Order in Fields

One of the most useful properties of the rational number system is the fact that the elements are ordered; $7 < \frac{25}{2}$, $\frac{-3}{2} < \frac{1}{5}$, $\frac{1}{1,000} < \frac{1}{999}$, and so on. For this reason, whenever the rational numbers are used for measurement (such as length, area, probability, or weight) measures in the same unit can be compared. For example, in an earlier dice tossing game you found that for a toss of two dice P(5 or 6 or 7 or 8 or 9) = $\frac{24}{36}$ and P(2 or 3 or 4 or 10 or 11 or 12) = $\frac{12}{36}$. The conclusion was that the player who wins with sum 5,6,7,8 or 9 would win in the long run because $\frac{12}{36} < \frac{24}{36}$.

The order relation "<" in (Q,+,·) has the following basic properties:

O 1. Transitive Property. For all a,b,c in Q, if a < b and b < c, then a < c.

O 2. Trichotomy Property. For each a in Q, exactly one of the following holds:

$a < 0, \qquad a = 0, \qquad 0 < a$

O 3. Additive Property. For all a,b,c in Q if a < b then

$a + c < b + c$.

O 4. Multiplicative Property. For all a,b,c in Q if $a < b$ and $0 < c$, then $ac < bc$.

We say that $(Q,+,\cdot)$ is an ordered field. Any field $(F,+,\cdot)$ for which there is an order relation "<" satisfying O 1 -- O 4 (as axioms) for elements in F is called an ordered field. We indicate this by "$(F,+,\cdot,<)$." In any ordered field the statements "$a < b$" and "$b > a$" are equivalent. ("$a < b$" is read "a is less than b" and "$b > a$" is read "b is greater than a.")

$$\frac{2}{3} < \frac{7}{8} \text{ is equivalent to } \frac{7}{8} > \frac{2}{3}.$$

What sort of theorems can be proven about ordered fields? As is often the case in mathematics, conjectured theorems appear in examination of specific situations. The following discussion exercises involving order in $(Q,+,\cdot,<)$ should suggest some theorems that are true in all ordered fields.

Discussion Exercises

In each of the following, choose the symbol "<" or ">" that completes the statement correctly.

1. (a) $\frac{7}{2}$ ____ $\frac{12}{3}$ (c) $\frac{-7}{2}$ ____ $\frac{-12}{3}$

   (b) 0 ____ $\frac{12}{3} - \frac{7}{2}$ (d) $\frac{2}{7}$ ____ $\frac{3}{12}$

2. (a) $\frac{-2}{3}$ ____ $\frac{5}{2}$ (b) $\frac{-6}{8} \cdot \frac{-2}{3}$ ____ $\frac{-6}{8} \cdot \frac{5}{2}$

3. (a) $\frac{1}{2}$ ____ $\frac{1}{3}$ (b) $\frac{-7}{3}$ ____ $\frac{-1}{4}$ (c) $\frac{1}{2} + \frac{-7}{3}$ ____ $\frac{1}{3} + \frac{-1}{4}$

4. (a) $\frac{2}{5}$ ____ $\frac{7}{8}$ (b) $\frac{8}{7} \cdot \frac{2}{5}$ ____ 1

5. $\left(\frac{-2}{3}\right)^2$ ____ 0

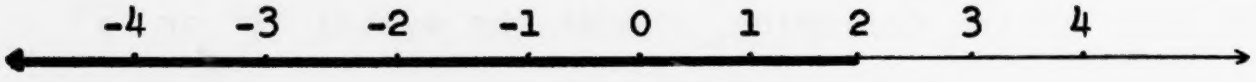
Now try formulating some tentative ordered field theorems. Several of your propositions will probably appear in the following sequence:

Elementary Inequality Theorems

The solution set of the inequation "$2x + 3 < 7$" in $(Q,+,\cdot,<)$ is easy to calculate:

1. $2x + 3 < 7$ implies $(2x + 3) + (-3) < 7 + (-3)$ [by property (O 3)].
2. $(2x + 3) + (-3) < 7 + (-3)$ implies $2x < 4$ [by associativity and arithmetic].
3. $2x < 4$ implies $\frac{1}{2}(2x) < \frac{1}{2}\cdot 4$ or $x < 2$ [by property (O 4)].

Thus if x satisfies "$2x + 3 < 7$," it also satisfies "$x < 2$," and you can check that the converse is true also. On a number line, the solution set is a ray.



But this open sentence was quite easy to solve; you might have guessed the answer. To deal with more intricate inequalities it is handy to have other methods of transforming inequalities into equivalent simpler inequalities.

Theorem OF 1. For all a,b in ordered field $(F,+,\cdot,<)$:

(a) $a < b$ if and only if $0 < b - a$

(b) $a < 0$ if and only if $0 < -a$

(c) $a < b$ if and only if $-b < -a$.

Proof. (a) First, if $a < b$ then $a + (-a) < b + (-a)$ by O 3. But $a + (-a) = 0$ and $b + (-a) = b - a$. Thus $a < b$ implies $0 < b - a$.

Conversely, if $0 < b - a$ then $0 + a < (b - a) + a$ and simplifying both sides we get $a < b$.

The proofs of (b) and (c) involve similar strategies.

Theorem OF 2. For all a,b,c,d in ordered field $(F,+,\cdot,<)$:

(a) $a > b$ and $c > d$ implies $a + c > b + d$.

(b) $a > 0$ and $b > 0$ implies $a + b > 0$.

Proof. Exercises

Theorem OF 3. For all a,b,c,d in ordered field $(F,+,\cdot,<)$:

(a) $a > 0$ and $b > 0$ implies $a\cdot b > 0$.

(b) $a > b$ and $c < 0$ implies $ac < bc$.

Proof. We prove part (b).

(b) $c < 0$ implies $0 < -c$. But then applying O 4, $a(-c) > b(-c)$ or $-(ac) > -(bc)$ or $ac < bc$ [by OF 1].

Theorem OF 4. For all a in ordered field $(F,+,\cdot,<)$, $a^2 > 0$ or $a^2 = 0$.

Proof. Exercise.

Theorems OF 1--4 are but a few of the many properties useful in dealing with inequalities. Others appear in the exercises that follow.

4.11 Exercises

1. In each of the following, insert the symbol "<," ">,"

"$\geq$" (means greater than or equal to), or "$\leq$" that makes a true statement for all a,b,c,d in an ordered field.

(a) $a \cdot b > 0$ and $a > 0$ implies b ____ 0.

(b) $a \cdot b < 0$ and $a > 0$ implies b ____ 0.

(c) $a > b > 0$ and $c > d > 0$ implies ac ____ bd.

(d) 1^2 ____ 0.

(e) 1 ____ 0.

(f) $a + c < b + c$ implies a ____ b.

(g) $a > 0$ and $ac > ab$ implies c ____ b.

(h) $a < 0$ and $ac > ab$ implies c ____ b.

(i) $a > 0$ and $b \geq 0$ implies a + b ____ 0.

(j) $a > 0$ and $b \geq 0$ implies $a \cdot b$ ____ 0.

(k) $a < 0$ and $b \geq 0$ implies $a \cdot b$ ____ 0.

2. Use the ordered field properties to transform each of the following inequalities to a simpler equivalent inequality.

   (a) $-7x + 3 < 14$

   (b) $3(x - 4) < 12(x + 5)$

   (c) $3x^2 - 5 < x^2 + 3$

3. Prove Theorem OF 1, part (b).

4. Prove Theorem OF 1, part (c).

5. Prove Theorem OF 2, part (a).

6. Prove Theorem OF 2, part (b).

7. Prove Theorem OF 3, part (a).

8. Prove Theorem OF 4.

9. For all a,b in ordered field $(Q,+,\cdot,<)$ if $0 < a < b$, there is an element t in Q such that $0 < t < 1$ and $a = tb$.

(a) Find t in case

(1) $a = 7$ and $b = 14$.

(2) $a = 12$ and $b = 20$.

(3) $a = \frac{9}{8}$ and $b = \frac{15}{11}$.

(b) State a rule for finding t in terms of a and b in any case.

10. For all a,b in ordered field $(Q,+,\cdot,<)$, if $0 < a < b$, there is an integer n such that $na > b$. This is the Archimedean Property of the rational numbers.

(a) Find a value for n in case

(1) $a = \frac{1}{2}$ and $b = 12$.

(2) $a = \frac{1}{1000}$ and $b = 37$.

(3) $a = \frac{2}{5}$ and $b = 136$.

(b) State a general rule for finding a value for n in terms of a and b.

11. Try to formulate a definition of absolute value that is valid in any ordered field.

12. Try to formulate a definition of positive and negative elements valid in any ordered field.

4.12 How Many Ordered Fields?

The definition of an ordered field, like the definition of field itself, suggests two questions. Why was the particular collection of properties O 1 -- O 4 chosen? What examples of ordered fields (other than the rational numbers) are familiar?

The first answer is easy -- the rational number system is ordered in a way that makes the chosen properties fundamental, and we would like order in other fields similar to that in $(Q,+,\cdot,<)$. The answer to the second question, however, takes the wind out of the argument just given. $(Q,+,\cdot,<)$ is the only orderable field we have studied so far!

The proof of this surprising fact is really quite easy. Take $(Z_5,+,\cdot)$ as an example. By Theorem OF 4 we know that if Z_5 is ordered $a^2 > 0$ for all $a \neq 0$ in Z_5. In particular, $1^2 = 1 > 0$. But if $1 > 0$ then

$$2 = 1 + 1 > 0 \qquad \text{(Theorem OF 2)}$$

$$\text{and } 3 = 1 + 2 > 0$$

$$\text{and } 4 = 1 + 3 > 0$$

$$\text{and } 0 = 1 + 4 > 0\ !$$

It is not difficult to generalize this result to any field $(Z_p,+,\cdot)$.

In the sections on solving equations and inequations that follow, attention is focused in the ordered field $(Q,+,\cdot,<)$. However, you will see that the techniques for solving equations depend only on field theorems and are thus applicable in the finite, non-ordered fields.

4.13 Equations and Inequations in $(Q,+,\cdot,<)$

The manufacturer of ZOND X Motorcycles wants to bring out a new model for the "65 and Over" set. He calculates that design, re-tooling, and advertising will involve a fixed cost of \$75,000 and then each cycle will cost \$165 for labor and materials. If the f.o.b. price is to be \$179.50, how many cycles must Mr. Zond make and sell to at least break even? To break even the number n of cycles must satisfy the condition.

(1) $75{,}000 + 165n = 179.50n$.

To make a profit, n must satisfy the inequation

(2) $75{,}000 + 165n < 179.50n$.

To advise the manufacturer, we must solve the equation (1) or the inequation (2); that is, we must find roster names for the elements in the domain of the variable which make the given equation or inequation true when they are used as replacements for the variable.

In earlier work you have had experience solving similar equations and inequations. The purpose of this section and the next several sections is to develop some systematic procedures (based on the properties of an ordered field) useful in solving several important classes of equations and inequations.

Before tackling Mr. Zond's problem, let's examine a slightly easier example

Example 1. Find the solution set of "$7x + 10 = 15$."

$7x + 10 = 15$ implies $7x = 15 - 10$

(Theorem 10(e))

implies $7x = 5$

(Arithmetic fact)

implies $x = \frac{5}{7}$

(Theorem 9(e))

At this stage we have proved that for any x in Q, $7x + 10 = 15$ implies $x = \frac{5}{7}$, or equivalently, $\{x\colon 7x + 10 = 15\} \subset \{x\colon x = \frac{5}{7}\}$

Another way of stating this result

is: The only possible rational number x such that $7x + 10 = 15$ is $\frac{5}{7}$. This does not guarantee that $\frac{5}{7}$ is a root (solution) of this equation. In order to establish this we must prove that $x = \frac{5}{7}$ implies that $7x = 10 = 15$.

$x = \frac{5}{7}$ implies $7x = 7\cdot\frac{5}{7}$ Left operation
implies $7x = 5$ Arithmetic fact
implies $7x + 10 = 5 + 10$ Right Operation
implies $7x + 10 = 15$ Arithmetic fact

So we have just proved that if x is in Q, then $x = \frac{5}{7}$ implies $7x + 10 = 15$, or equivalently, $\{x\colon x = \frac{5}{7}\} \subset \{x\colon 7x + 10 = 15\}$.

The two proofs together now give us that

$\{x\colon x = \frac{5}{7}\} = \{x\colon 7x + 10 = 15\}$

In the last proof we had to show that

$\{x\colon x = \frac{5}{7}\} \subset \{x\colon 7x + 10 = 15\}$ and did so by a chain of implications. Since $\{x\colon x = \frac{5}{7}\} = \{\frac{5}{7}\}$, it would have been sufficient to prove that $\frac{5}{7} \in \{x\colon 7x + 10 = 15\}$. But $7\cdot\frac{5}{7} + 10 = 15$ and thus the statement is proved. We call this method "the check method" since in essence we plugged "$\frac{5}{7}$" into the equation for "x" to see if it "worked."

Example 2. Find the solution set for the equation

$$\frac{2}{3}x - \frac{5}{6} = 7.$$

$\frac{2}{3}x - \frac{5}{6} = 7$ implies $\frac{2}{3}x = 7 + \frac{5}{6}$

implies $x = (7 + \frac{5}{6})\cdot\frac{3}{2}$

implies $x = \frac{47}{4}$

Since $\frac{47}{4}$ "checks" we have as solution set $\{\frac{47}{4}\}$.

Example 3. Find the solution set of the equation

"$13 - 2x = \frac{1}{3}x - 4x$."

(1) $13 - 2x = \frac{1}{3}x - 4x$ implies

$13 - 2x = -\frac{11}{3}x$

implies $13 = 2x - \frac{11}{3}x$

implies $13 = -\frac{5}{3}x$

implies $\frac{^-39}{5} = x$.

(2) Check: $13 - 2(\frac{^-39}{5}) = \frac{1}{3}(\frac{^-39}{5}) - 4(\frac{^-39}{5})$.

(3) The solution set is $\{\frac{^-39}{5}\}$.

With these examples under your belt, Mr. Zond's problem should be a snap.

(1) $75{,}000 + 165n = 179.50n$ if and only if

$75{,}000 = 179.50n - 165n$

(2) $75{,}000 = 179.50n - 165n$ if and only if

$75{,}000 = 14.50n$

(3) $75{,}000 = 14.50n$ implies $n \approx 5172.4$.

The only question is whether or not such a solution makes sense. It says Mr. Zond should make 5172.4 motorcycles! We can do better with the inequation.

(1) $165n + 75{,}000 \leq 179.50n$ implies

$75{,}000 \leq 14.50n$ [Add $-165n$ to both sides by O 3.]

(2) $75{,}000 \leq 14.50n$ implies $\frac{1}{14.50} \cdot 75{,}000 \leq n$

[Multiply both sides by $\frac{1}{14.50}$ by O 4]

(3) Or $5172.4 \leq n$.

Thus Mr. Zond will profit on any number of cycles greater than 5172.4. The solution set of the inequation is $\{n\colon 5172.4 \leq n\}$.

There are two important aspects of this example. First the solution set is infinite and cannot be given a roster name. Second, the strategy used in solving the inequation is very similar to that used in solving the corresponding equation.

In the Zond problem we first analyzed the problem to obtain an equation from the given information in which the variable corresponded to the quantity which we wished to find, "n" for the number of cycles. This mathematical equation was solved. Then the root of the equation was interpreted as the quantity required by the problem. Thus, when solving such a problem we go from a "real-life" or "physical" situation to an equation in a mathematical system. The properties of the mathematical system are used to find the root of the given equation in the system and this root is then interpreted in terms of the given problem. This is a brief sketch of a process that is constantly recurring when a mathematical model is used to solve problems from the real world.

4.14 Exercises

1. For each of the following, write an expression of the form "$ax + b$" or "$ax^2 + bx + c$" that is equivalent to the given expression.

   (a) $(3x - 7) + 5x$
   (b) $\frac{5}{2} + (17x - 32x)$
   (c) $\frac{2}{3}x - (7x - 8x)$
   (d) $8 + 5x^2 - \frac{2}{3} - 11x^2$
   (e) $17 + 11x - 23x + 43 - \frac{7}{2}x$
   (f) $8(x^2 - 3x) + x(7 + x)$

2. Solve each of the following equations in $(Q,+,\cdot)$.

(a) $3x + 5 = 3$

(b) $\frac{2}{3} - \frac{5}{8}x = \frac{5}{6}$

(c) $18 = x \cdot \frac{43}{2}$

(d) $8x - 11 = \frac{7}{9} + 7x$

(e) $7(x - 5) = x(5 - 7)$

(f) $13x + 7(3 - x) = 12x - \frac{5}{6}$

(g) $\frac{2}{3}x + \frac{5}{6} = 7$

(h) $7x - 8x + 9x - 10x = 7 - 8 + 9 - 10$

3. Solve each of the following inequations in $(Q,+,\cdot,<)$.

(a) $3x < \frac{27}{12}$

(b) $-7x < \frac{5}{8}$

(c) $8 - 3x < 12$

(d) $\frac{2}{3} < 15x - 4$

(e) $7(x - \frac{2}{3}) < 4x$

(f) $3x + 5 < 3$

(g) $18 < \frac{43}{2}x$

(h) $7x - 8x + 9 - 10 < 9x - 10x + 7 - 8$

4. Solve each of the following equations in $(Z_{29},+,\cdot)$.

(a) $15x + 23 = 8$

(b) $15x - 23 = -17$

(c) $8x + 5 = 13 - 22x$

(d) $8(x - 2) = 19$

5. Zond's competitor designed a cheaper cycle which costs $90 to make and sells for $99.50. If the competitor cuts his fixed cost to $45,000, what is his break-even point in sales?

4.15 Solving Quadratic Equations

None of the equations we have considered thus far have contained symbols such as "x^2," "c^2," "y^2," etc. and each equation has involved only a single variable. These equations are examples of linear equations in a single variable. Without attempting to define such equations precisely we note only that for all such equations there was an equivalent open sentence of the type "$ax + b = c$ and $a \neq 0$." The roster name of the solution set is $\{\frac{c - b}{a}\}$.

There are certain equations involving "x^2" that can be solved at this time. For instance, "$x^2 = 16$" has solution set $\{4, -4\}$. The equation "$x^2 - \frac{9}{4} = 0$" has solution set $\{\frac{3}{2}, -\frac{3}{2}\}$. The equation "$x^2 + \frac{3}{4}x = 0$" has solution set $\{0, -\frac{3}{4}\}$ which is determined as follows:

(1) $x^2 + \frac{3}{4}x = 0$ if and only if $x(x + \frac{3}{4}) = 0$

(2) $x(x + \frac{3}{4}) = 0$ if and only if $x = 0$ or $(x + \frac{3}{4}) = 0$

(3) $(x + \frac{3}{4}) = 0$ if and only if $x = -\frac{3}{4}$.

Furthermore, the equation "$(x + \frac{7}{8})(3x - \frac{1}{2}) = 0$" has solution set $\{-\frac{7}{8}, \frac{1}{6}\}$, obtained by reasoning similar to that just above. But this last equation is a queer duck. It has two solutions -- not one like the linear equations--but does not seem to involve any "x^2" terms.

The following calculation involving the distributive property shows that the equation is equivalent to one that does involve "x^2."

(1) $(x + \frac{7}{8})(3x - \frac{1}{2}) = 0$ if and only if

$(x + \frac{7}{8}).3x - (x + \frac{7}{8}).\frac{1}{2} = 0$ [Theorem 12]

(2) if and only if $3x^2 + \frac{21}{8}x - \frac{1}{2}x - \frac{7}{16} = 0$

[Theorem 2 and the commutative and distributive properties in a field]

(3) if and only if $3x^2 + \frac{17}{8}x - \frac{7}{16} = 0$.

This observation can be generalized to solve a wide range of quadratic equations in a single variable, those involving "x^2" and no higher power of "x."

Example 1. "$x^2 + 6x + 8 = 0$" has solution set $\{-4, -2\}$ since the equation is equivalent to "$(x + 4)(x + 2) = 0$" (check this as above) and the latter equation is satisfied if and only if $x + 4 = 0$ or $x + 2 = 0$.

Example 2. "$x^2 + 3x - 10 = 0$" has solution set $\{-5, 2\}$ since it is equivalent to "$(x + 5)(x - 2) = 0$."

These examples make it clear that solving quadratic equations of the form "$ax^2 + bx + c = 0$" will be easier if you develop some facility in writing these equations in factored form.

An expression of the form "$(x + a)(x + b)$" is equivalent to "$x^2 + (a + b)x + ab$" as the following calculation shows.

$$\begin{aligned}(x + a)(x + b) &= (x + a)x + (x + a)b \\ &= x^2 + ax + bx + ab \\ &= x^2 + (a + b)x + ab\end{aligned}$$

Therefore to factor an expression in the form "$x^2 + cx + d$," we must find two numbers, a and b, such that $a + b = c$ and $a \cdot b = d$.

Example 3. For all x, $x^2 + 11x + 24 = (x + 8)(x + 3)$ Since $8 + 3 = 11$ and $8 \cdot 3 = 24$.

Example 4. For all x, $x^2 - \frac{2}{3}x + \frac{1}{9} = (x - \frac{1}{3})(x - \frac{1}{3})$ since $-\frac{1}{3} + (-\frac{1}{3}) = -\frac{2}{3}$ and $(-\frac{1}{3})(-\frac{1}{3}) = \frac{1}{9}$.

Example 5. For all x, $x^2 - 25 = (x - 5)(x + 5)$ since $5 + (-5) = 0$ and $(5)(-5) = -25$.

4.16 Exercises

1. Write each of the following expressions in an equivalent "$ax^2 + bx + c$" form. In some cases a, b, or c might be zero.

   (a) $(x + 7)(x + 11)$

   (b) $(x - \frac{1}{2})(x + \frac{5}{8})$

   (c) $(x - 3)(x - 3)$

   (d) $(x - 8)(x + 22)$

   (e) $(x + 8)(x - 22)$

   (f) $(8 - x)(22 - x)$

   (g) $(x + 3)(x - 3)$

   (h) $(x + 5)(x - 4)$

   (i) $(3x + 2)(4x + 5)$

   (j) $(\frac{5}{6}x - 10)(\frac{12}{7}x + 4)$

2. Factor each of the following expressions.

   (a) $x^2 + 9x + 20$

   (b) $x^2 - 9x + 20$

   (c) $x^2 + x - 20$

   (d) $x^2 - x - 20$

   (e) $x^2 - 8x - 20$

   (f) $x^2 + 12x + 20$

3. Solve each of the following equations.

   (a) $x^2 - 11x = 0$

   (b) $(x - \frac{2}{3})(3x + 4) = 0$

   (c) $3x + 4x^2 = 0$

   (d) $x^2 - \frac{16}{25} = 0$

   (e) $(x - 8)(x + 8) = 0$

   (f) $4x^2 - 3x = 7x^2 + 10x$

4. Solve each of the following equations.

   (a) $x^2 + 8x + 15 = 0$

   (b) $x^2 - 6x + 8 = 0$

   (c) $x^2 + 11x = 26$

   (d) $x^2 + 6x + 9 = 0$

   (e) $x^2 - 6x + 9 = 0$

   (f) $x^2 - 4x - 12 = 0$

   (g) $x^2 + 4x - 12 = 0$

   (h) $x^2 - 7x + 12 = 0$

5. Solve each of the following equations.

   (a) $3x - 7 = 12$

   (b) $3x^2 - 7x = 12x$

   (c) $x - \frac{4}{5} = \frac{5}{10}x - \frac{1}{10}$

   (d) $7x^2 - x = 7x^2 + 3$

   (e) $8x + 3 - 4x = 7x - 12$

*6. Find the solution set of each of the following inequations. [Hint: First solve the corresponding equations, locate the roots on a number line, and then try numbers in the three regions determined.]

(a) $x^2 + 3x + 2 \leq 0$

(b) $x^2 + 5x - 14 > 0$

(c) $x^2 - 25 < 0$

(d) $3x^2 - 4x + 1 < 0$

7. Solve the following equations where the domain of x is $(Z_{11},+,\cdot)$.

(a) $x^2 - 4 = 0$ (c) $x^2 + 3x + 4 = 0$

(b) $x^2 + 3x + 2 = 0$ (d) $x^2 - 3 = 0$

Note: 5 is a root of (d) in $(Z_{11},+,\cdot)$ but is not a root in $(Q,+,\cdot)$. Can you find another root of $x^2 - 3 = 0$ in $(Z_{11},+,\cdot)$? Does (d) have any roots in $(Q,+,\cdot)$?

*8. Try to solve each of the following equations by factoring. Since the coefficient of x^2 is not 1 in the quadratic expressions, you might need factors of the form $(ax + b)(cx + d)$.

(a) $3x^2 = 14x + 8 = 0$ (c) $4x^2 + 6x + 2 = 0$

(b) $4x^2 - 7x - 2 = 0$ (d) $9x^2 - 25 = 0$

4.17 Summary

1. A field is any two-fold operational system $(F,+,\cdot)$ which has the nine properties enumerated in Section 4.1. The structure of a field can be summarized as follows.

(a) $(F,+)$ is a commutative group with identity 0.

(b) $(F\setminus\{0\},\cdot)$ is a commutative group with identity 1.

(c) Multiplication is distributive over addition; that is, for all a,b,c in F

$a(b + c) = (ab) + (ac)$.

2. The most familiar examples of fields are the rational number system, $(Q,+,\cdot)$, and the finite systems $(Z_2,+,\cdot)$, $(Z_3,+,\cdot)$, $(Z_5,+,\cdot)$, and $(Z_7,+,\cdot)$. Of these, only $(Q,+,\cdot)$ can be ordered. In Q there is a relation, $<$, defined by Axioms O 1 -- O 4, which are listed in Section 4.10.

3. Some of the major field theorems are:

   (a) For all a in F, $a \cdot 0 = 0$.

   (b) For all a,b in F, $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

   (c) For all a,b in F, $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

   (d) Every equation of the form "$ax + b = c$" has solution set $\{\frac{c - b}{a}\}$ if $a \neq 0$.

4. Some of the major ordered field theorems are:

   (a) If a and b are in F, then $a > 0$ and $b > 0$ implies $a + b > 0$ and $ab > 0$.

   (b) If a,b, and c are in F, then $a > b$ and $c < 0$ implies $ac < bc$.

   (c) If a, b, c, and d are in F, then $a > b$ and $c > d$ implies $a + c > b + d$.

   (d) For all x in F, $x^2 \geq 0$.

5. In any field $(F,+,\cdot)$ subtraction and division are defined as follows:

   (a) If a and b are in F, then $a - b = a + (-b)$

   (b) If a and b are in F and $b \neq 0$, then

   $a \div b = \frac{a}{b} = a \cdot b^{-1}$.

Many properties of subtraction and division follow from these definitions and the properties of $(F,+,\cdot)$. Some of these are (where a, b, and c are in F):

(1) $a + b = c$ if and only if $a = c - b$

(2) For $b \neq 0$, $a \div b = c$ if and only if $a = b\cdot c$

(3) $0 - a = -a$

(4) For $b \neq 0$, $1 \div b = \frac{1}{b} = b^{-1}$.

6. Summary item 3(d) allows us to find exactly one root for each linear equation in one variable whose domain is F. Also, item 3(b) allows us to find roots for some equations involving "x^2" such as "$x^2 - 4 = 0$," "$x^2 - 3x - 10$," $= 0$ and "$(x - 2)(x + 3) = 0$."

4.18 Review Exercises

1. Evaluate each of the following where $a = 2$, $b = 5$, and $c = 3$ in $(Z_7,+,\cdot)$.

(a) $a \div b$ (c) $a^2 - 4bc$

(b) $b\cdot(-c)^{-1}$ (d) $a^{-1}\cdot b^{-1}$

2. Evaluate each of the following where $a = \frac{2}{3}$, $b = -\frac{7}{5}$, $c = 15$ in $(Q,+,\cdot)$.

(a) $a \div b$ (c) $a^2 - 4bc$

(b) $b\cdot(-c)^{-1}$ (d) $a^{-1}\cdot b^{-1}$

3. Prove each of the following theorems for any field $(F,+,\cdot)$.

(a) For all a in F, $-(-(-a)) = -a$.

(b) For all a,b,c in F $(a \neq 0)$, if $a\cdot b = a\cdot c$ then $b = c$.

(c) For all x,a,b in F. $(x - a)(x - b) = x^2 - ax - bx + ab$.

(d) For all x,a in F, $(x - a)(x + a) = x^2 - a^2$.

4. Prove each of the following theorems for the ordered field $(Q,+,\cdot,<)$.

   (a) For all a,b, $a < b$ implies $\frac{a+b}{2} < b$.

   (b) For all a,b, $a < 0$ and $b > 0$ implies $ab < 0$.

   (c) For all a, $a > 0$ implies $\frac{1}{a} > 0$.

5. Solve each of the following equations in $(Q,+,\cdot)$.

   (a) $\frac{7}{10}x - 11 = 23$

   (b) $\frac{1}{2}x + 5 = 11x - 13$

   (c) $x^2 - \frac{49}{144} = 0$

   (d) $3x^2 - 7x = 0$

   (e) $x^2 + 17x + 72 = 0$

   (f) $2x^2 + 10x + 12 = 0$

Chapter 5

THE REAL NUMBER SYSTEM

5.1 The Equation $x^2 = 2$

The rational number system, $(Q,+,\cdot)$, is an ordered field, the second step in an expension of the familiar whole number system, $(W,+,\cdot)$. In $(W,+,\cdot)$ neither addition nor multiplication satisfy the group properties and, as a result, simple equations like $x + a = b$ and $x\cdot a = b$ have no whole number solutions. Extension of W to Z and then to Q yielded an operational system without these inadequacies; both $(Q,+)$ and $(Q\setminus\{0\},\cdot)$ are groups, and in the system $(Q,+,\cdot)$ every equation of the form

$$a\cdot x + b = c$$

has a unique solution (unless $a = 0$).

Many more complicated equations have solutions in $(Q,+,\cdot)$. For example, $3x - 7x + 23 = 45 - 18x$ has solution set $\{\frac{11}{7}\}$ and $x^2 + 6x + 8$ has solution set $\{-2,-4\}$. But what is the solution set of the equation $x^2 = 2$ in $(Q,+,\cdot)$? This equation certainly looks much simpler than the previous ones. How would you begin to solve this problem?

You might guess at a whole number. But $1^2 < 2$ and $2^2 > 2$, so you would be forced to guess again. A likely second guess would be some rational number between 1 and 2. Try $x = \frac{3}{2} = 1.5$.

$$\left(\frac{3}{2}\right)^2 = \frac{9}{4} = 2.25.$$

Since $\frac{3}{2}$ is too large, you might try $\frac{5}{4} = 1.25$ or $\frac{7}{5} = 1.4$ next.

$$\left(\frac{5}{4}\right)^2 = \frac{25}{16} \qquad\qquad \left(\frac{7}{5}\right)^2 = \frac{49}{25}$$

$\frac{49}{25}$ is close to 2, so your next choice might be close to $\frac{7}{5}$.

You might feel that you could find a rational number whose square is 2, given a few more guesses. It may surprise or even shock you to learn than, no matter how many guesses you make, you will never find a rational number whose square is 2. The solution set $S = \{x: x \in Q \text{ and } x^2 = 2\}$ is empty.

In order to convince you that this solution set is empty, let us assume that it is possible to find an $x \in Q$ such that $x^2 = 2$ and show that this assumption leads to a contradiction. It is a principle of logic, which you have encountered before, that if an assumption leads to a contradiction, the assumption must be false. Thus, if we reach a contradiction with our assumption, we will be able to conclude that there is no $x \in Q$ such that $x^2 = 2$.

Theorem: $\{x \in Q: x^2 = 2\} = \emptyset$

Proof: Assume there is an $x \in Q$ such that $x^2 = 2$. Then there are positive integers p and q, with $q \neq 0$, such that $x = \frac{p}{q}$. By substitution in "$x^2 = 2$", we get $(\frac{p}{q})^2 = \frac{p^2}{q^2} = 2$. This tells us that $p^2 = 2q^2$. Imagine the complete factorization of p into primes. For example, if $p = 600$, then $p = 2^3\cdot 3\cdot 5$; if $p = 252$, then $p = 2^2 \cdot 3^2 \cdot 7$. Now consider the complete factorization of p^2 into primes. If $p = 600$, then $p^2 = (600)(600) = (2^3\cdot 3\cdot 5^2)(2^3 . 3\cdot 5^2) = 2^6\cdot 3^2\cdot 5^4$, whereas if $p = 252$, then $(252)^2 = (252)(252) = (2^2 . 3^2\cdot 7)(2^2 . 3^2\cdot 7) = 2^4\cdot 3^4\cdot 7^2$. In general, no matter how many factors of 2 that the prime factorization of p contains, p^2 contains

> twice as many factors of 2 in its prime factorization. Thus p^2 must contain an even number (possibly zero) of factors of 2 in its complete factorization into primes. Similarly, q^2 must contain an even number (possibly zero) of factors of 2 in its complete factorization into primes. Thus $2q^2$, since it contains one more factor of 2 than q^2, it must contain an odd number of factors of 2 in its complete factorization into primes. Now, if $p^2 = 2q^2$, the Unique Factorization Property would require that both p^2 and $2q^2$ have the same factorizations into primes; in particular, both should contain the same number of factors of 2. But p^2 contains an even number of factors of 2 while $2q^2$ contains an odd number of factors of 2.

The assumption, that there is a rational number whose square is 2, led to a statement which contradicts an established principle of mathematics. The assumption must therefore be false. There is no rational number whose square is 2.

Just as the equation $x + 5 = 4$ had an empty solution set in $(W,+,\cdot)$ and $2x = 5$ had an empty solution set in $(Z,+,\cdot)$, the equation $x^2 = 2$ has an empty solution set in $(Q,+,\cdot)$. The extension to $(Q,+,\cdot)$ is not sufficient to solve all equations that might reasonably occur. The next section presents a very different inadequacy of the rational number system, one with a strong geometrical flavor.

5.2 Exercises

1. For each of the following natural numbers n, find the complete factorization into primes of n and of n^2. How many factors of 3 are in each factorization? What relationship do you observe?

   (a) 20 (b) 42 (c) 2250 (d) 270 (e) 891

2. (a) Use the Unique Factorization Property to show that the solution set of each of the following equations is empty in $(Q,+,\cdot)$.

   (i) $x^2 = 3$ (ii) $x^2 = 5$ (iii) $x^2 = 6$

   (b) Why doesn't the same reasoning apply to the equation $x^2 = 4$?

3. Find the solution set of each of the following equations in $(Q,+,\cdot)$.

   (a) $x^2 + 12^2 = 13^2$ (c) $8^2 + y^2 = 17^2$ (e) $1^2 + 1^2 = x^2$

   (b) $3^4 + 4^2 = a^2$ (d) $2^2 + x^2 = 2^2$

4. Find two elements in each of the following sets.

   (a) $\{x: x \in Q \text{ and } |2 - x^2| < .1\}$

   (b) $\{x: x \in Q \text{ and } |2 - x^2| < .01\}$

   (c) $\{x: x \in Q \text{ and } |3 - x^2| < .1\}$

   (d) $\{x: x \in Q \text{ and } |3 - x^2| < .01\}$

5.3 The Measuring Process

In Figure 5.1, you will find a square whose side has a length of 1 unit, say 1 centimeter. What is the length of the

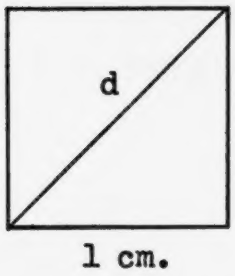


Figure 5.1

diagonal, labeled "d", in the diagram? Mathematicians have known since 500 B.C. that there is a relationship among the lengths of the three sides of a right triangle. If "a" and "b" represent the lengths of the two shorter sides of a right triangle and "c" represents the length of the hypotenuse, then $c^2 = a^2 + b^2$. This is called the Pythagorean property. Applying this property to one of the two right triangles in the square above, we see that

$$d^2 = 1^2 + 1^2$$

$$d^2 = 2.$$

The length of the diagonal is, therefore, a number whose square is 2. However, in Section 5.1, we proved that $\{x: x \in Q \text{ and } x^2 = 2\} = \emptyset$. This means that no element in Q is the measure of d. What does this result imply? Shall we say that the diagonal of this square has no length? Would you be willing to accept this? In order to shed light on this situation, we examine the process of measuring length of a line segment in terms of a given unit length.

Suppose we want to measure the length of a line segment $\overline{AB}$ using a unit segment u̲ of length one centimeter. First, start at point A and lay off a string of segments along $\overline{AB}$, each congruent to the unit segment, until the end point of a segment falls on or passes B. (See Figure 5.2.)

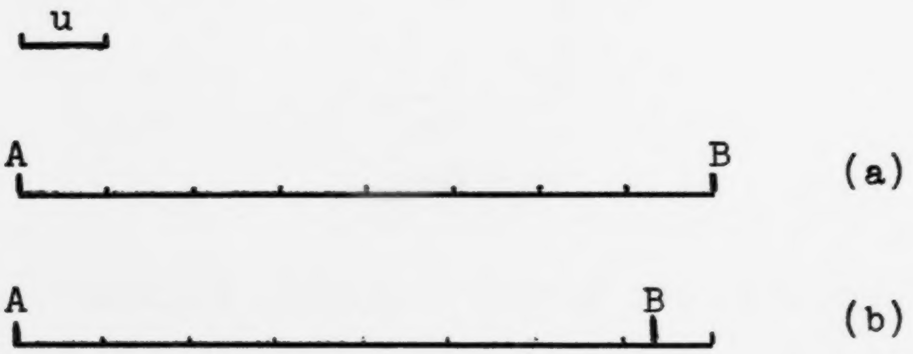


Figure 5.2

If (as in 5.2a) some collection of segments exactly covers $\overline{AB}$, count the number of segments used. This is the length in centimeters of $\overline{AB}$; in example 5.2a the length is 8 centimeters. If (as in 5.2b) the last segment used goes beyond B, count the number of unit segments up to this last. This number is not the length of $\overline{AB}$, but a first approximation to the desired length; in the case of 5.2b the lower approximation is 7 centimeters.

If the first step in the measuring process produced only an approximation to the length of $\overline{AB}$, label the end point of the last counted segment "D". (See Figure 5.3.)

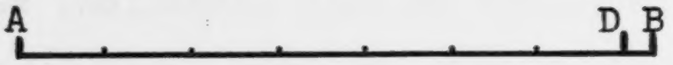


Figure 5.3

The length of $\overline{DE}$ is less than one centimeter. To obtain a measure of the length of $\overline{DB}$ we use a new unit p with length $\frac{1}{10}$ centimeter. We start at D and lay off a string of segments along $\overline{DB}$, each congruent to new unit p, until the end point of a segment falls on or passes B. (See Figure 5.4.)

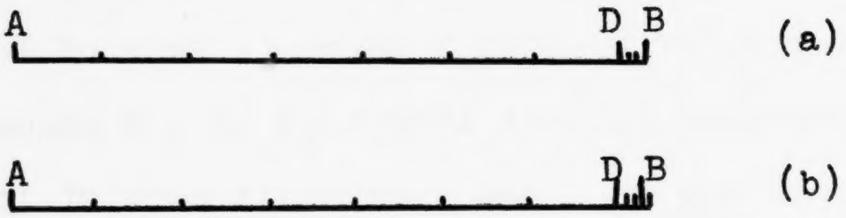


Figure 5.4

If (as in 5.4a) the resulting collection of segments covers $\overline{DB}$ exactly, count the number of segments used. This is the length in tenths of centimeters of $\overline{DB}$ and combined with the measure of $\overline{AD}$ it gives the length of $\overline{AB}$. In the case of 5.4a, the length of $\overline{DB}$ is $\frac{3}{10}$ centimeters and the length of $\overline{AB} = 7 + \frac{3}{10} = 7.3$ centimeters.

If (as in 5.4b) the last segment goes beyond B, count the number of unit segments used up to this last. This number is not the length of $\overline{DB}$, but an approximation. Together with the length of $\overline{AD}$ obtained in the first phase of measurement, it gives a second approximation to the length of $\overline{AB}$. In the case of 5.4b the approximation to length $\overline{DB}$ is $\frac{2}{10}$ centimeter and the approximation to length $\overline{AB}$ is $7 + \frac{2}{10} = 7.2$ centimeters.

If this measuring process has still not produced an exact length measure for $\overline{AB}$, we label the end point of the last segment "E" and repeat the procedure with a unit q of length $\frac{1}{100}$ centimeter. At the end of this step we might get an exact measure for the length of $\overline{AB}$ or a third approximation.

In the next few sections, you will see that if we continue measuring AB by this process, we encounter one of two possibilities:

(1) The process ends after a finite number of measurements, in which case we have found the length of $\overline{AB}$. For example, if we used 7 segments each of length 1 cm., 2 segments each of length $\frac{1}{10}$ cm., 4 segments each of length $\frac{1}{100}$ cm., and 3 segments each of length $\frac{1}{1000}$ cm. in order to reach just to point B, we have the centimeter measure of $\overline{AB}$ is $7 + \frac{2}{10} + \frac{4}{100} + \frac{3}{1000} = 7.234$. Notice that $7.234 = \frac{7234}{1000}$ and is therefore a rational number. If the measuring process does end, as in this example what can you say about the length?

(2) The measuring process does not end; it produces an infinite set of rational numbers each of which is viewed as an approximation to the length of $\overline{AB}$. These approximations would look as follows:

First approximation: k (k is the number of segments of length 1 cm. used.)

Second approximation: $k + \frac{a_1}{10}$ (a_1 is the number of segments of length $\frac{1}{10}$ cm. used.)

Third approximation: $k + \frac{a_1}{10} + \frac{a_2}{100}$

Fourth approximation: $k + \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000}$.

If the measuring process does not end, how could we then determine the length of $\overline{AB}$? Surely, we want to assign a length to this segment. Is this length in centimeters expressible by some number in the field of rational numbers? The problem considered in Section 5.5 is developing a procedure which will allow us to use the set of rational numbers produced by the measuring process to assign a length to the segment.

5.4 Exercises

1. Each of the following rational numbers represents the centimeter length of a line segment. For each number, give the set of rational numbers produced by the measuring process; explain what each digit in the number represents.

   Example: 7.031

   The measuring process produces the set: {7, 7.0, 7.03, 7.031}. 7 segments each of length 1 cm.; 0 segments each of length $\frac{1}{10}$ cm.; 3 segments each of length $\frac{1}{100}$ cm.; 1 segment of length $\frac{1}{1000}$ cm.

   (a) 6.1 (b) .32 (c) 47.503 (d) 2.15398

2. For each of the following sets, find a number in Q which is greater than or equal to every element in the set. (Assume the patterns in b and c continue.)

   (a) {3, 3.7, 3.72, 3.728} (c) {1, 1.7, 1.71, 1.717, 1.7171, ...}

   (b) {0, .9, .99, .999, .9999, ...} (d) $\emptyset$

3. For each of the sets listed in Exercise 2, find the smallest number in Q which is greater than or equal to every element in the set.

4. Use the Pythagorean relationship "$c^2 = a^2 + b^2$" to find the missing length in each of the following:

   (a) $b = 3, c = 5$ (b) $a = 10, c = 26$

   (c) $a = 7, b = 24$ (d) $a = 1, b = 1$

   (e) $b = 15, c = 17$

5. Find all integers x which satisfy the following inequations:

   (a) $0 < \frac{x}{10} < \frac{1}{3}$ (c) $0 < \frac{x}{100} < \frac{1}{30}$

   (b) $0 < \frac{x}{100} < \frac{1}{3}$ (d) $0 < \frac{x}{1000} < \frac{1}{300}$

5.5 The Length of a Line Segment

The measuring process, when applied to a particular line segment, produces a set of rational numbers. If the process ends, then this set is finite and includes the length of the segment. If the process does not end, then the set is infinite and each rational number produced may be viewed as an approximation to the length of the segment. We now seek a general mathematical procedure which will allow us to determine the length of a segment using this set of rational numbers generated by the measuring process, whether finite or infinite. Let

$$T = \{1, 1.5, 1.52, 1.528\ldots\},$$

where T may be finite or infinite, be one such set arising from the measuring process. Although we cannot establish a pattern that will enable us to state the next element in T, we can say several things about it. Each element in T is a rational number which cannot exceed the actual length of the segment being measured. (Why?) If we call the length "ℓ" then, for each t in T, we know that $t \leq \ell$. A number that is greater than or equal to each element of a set is called an upper bound of the set.

Definition 1. Let $(F,+,\cdot,<)$ be an ordered field and let $S \subset F$. An element b in F is an upper bound of S if and only if for each $s \in S$, $s \leq b$. If such an upper bound exists, then S is said to be bounded from above.

The length of a segment is an upper bound for the set of rational numbers which arises from the measuring process.

Consider set T listed above. Though we have listed only 4 elements in T, we may say that 2 is an upper bound of this set since every element in T must be less than 2. (Why?) But every element in T is also less that 10 or 20 or even 1.6. So we see that if a set has one upper bound, it has many upper bounds. The length of a segment is, therefore, one of the many upper bounds that exist for a particular set of rational numbers arising from the measuring process.

Which upper bound shall we choose? Suppose b_1 and b_2 are any two different upper bounds for set T. Thus, if $t \in T$ then, $t \leq b_1$ and $t \leq b_2$. Which of the two upper bounds is "closer" to the elements of T? In other words, which of the upper bounds, b_1 or b_2, differs from the elements of T by a small amount? Isn't it reasonable to expect the smaller of the two upper bounds to be "closer" to the elements of T? What we are looking for is the least upper bound of set T.

Definition 2. b is the least upper bound of set T if and only if:

(1) b is an upper bound of T.

(2) If b' is any upper bound of T, then $b \leq b'$. [least upper bound is usually abbreviated "l.u.b."]

The first property says that if b is to qualify as the least upper bound of T, it must first be an upper bound of T. The second property tells us that in order for b to be the least of the upper bounds of T, it cannot exceed any other upper bound.

The preceding discussion suggests the following definition of the length of a line segment:

Definition 3. The length of a line segment is the least upper bound of the set of rational numbers which arises from applying the measuring process to the segment.

Now we have a procedure for finding the length of any given line segment:

(1) Apply the measuring process to the line segment. If the process ends, it generates a finite set S of rational numbers, one of which is the actual length of the segment. If the process does not end, it generates an infinite set S of rational numbers, each of which is an approximation to the length of the segment.

(2) In either case the least upper bound of set S is the length of the segment. In Section 5.7 we will consider several concrete applications of this procedure.

5.6 Exercises

1. Find an upper bound in Q for each of the following sets (not all of which were obtained by the measuring process)

   (a) $\{x: x \in Q \text{ and } x^2 = 16\}$
   (b) $\emptyset$
   (c) $\{1, 1.1, 1.2, \ldots, 1.9\}$
   (d) $\{1, 2, 3, 4, \ldots\}$
   (e) $\{2, 2.3, 2.37, 2.371, 2.3718, \ldots\}$
   (f) $\{\frac{1}{2}, -\frac{3}{4}, \frac{4}{5}, -\frac{5}{6}, \frac{6}{7}, -\frac{7}{8}, \ldots\}$

2. Find the least upper bound in Q of each of the sets in Exercise 1.

3. Each of the following sets consists of the rational numbers produced by the measuring process as approximations to the

length of a line segment. In each case, find the actual length, in Q, of the segment

(a) $\{2\}$ (c) $\{7, 7.1, 7.14, 7.145\}$

(b) $\{.3, .33, .333, .3333, \ldots\}$ (d) $\{1, 1.6, 1.66, 1.666, 1.6668\}$

4. Let A and B be subsets of Q. Show that if A and B are both bounded from above, then

   (a) $A \cup B$ is bounded from above.

   (b) $A \cap B$ is bounded from above.

   Give an example to illustrate each of these statements.

5. Let $A \subset Q$. Prove that if x is an upper bound of A in Q and if $y \in Q$ and $y > x$, then y is an upper bound of A.

6. Let $A \subset Q$. Let $x, y \in Q$. Show that if x is a least upper bound of A and y is a least upper bound of A, then $x = y$.

5.7 Three Illustrative Cases

In this section, you will encounter three cases that illustrate the use of least upper bounds to find the length of a line segment. These cases also reflect different problems in assigning a numerical value to this length.

Case 1. The measuring process ends.

Suppose the measuring process, when applied to a line segment $\overline{CD}$, produces the following finite set of rational numbers:

$$S = \left\{\begin{array}{l} 4, \\ 4 + \frac{7}{10}, \\ 4 + \frac{7}{10} + \frac{3}{100}, \\ 4 + \frac{7}{10} + \frac{3}{100} + \frac{5}{1000}, \\ 4 + \frac{7}{10} + \frac{3}{100} + \frac{5}{1000} + \frac{8}{10000} \end{array}\right\}$$

In decimal fraction notation, we can display set S as

$$S = \{4, 4.7, 4.73, 4.735, 4.7358\}.$$

Notice that set S contains only 5 rational numbers. This means that in the fifth step of the measuring process, when laying off a string of congruent segments, each of length $\frac{1}{10000}$ centimeters, the last point falls directly on point D of segment $\overline{CD}$, eliminating the need for further measurements. The length, in centimeters, of $\overline{CD}$ is 4.7358.

What is the least upper bound of set S? It is easy to see that 4.7358 is an upper bound of S and that if x is any upper bound, then $4.7358 \leq x$. This means that 4.7358 is the least upper bound of S. If A is any non-empty finite set of rational numbers and if a is the greatest element in A, then a is the least upper bound of A.

Case 1 shows that if the measuring process produces a finite set S of rational numbers, then the greatest rational number in S is both the length of the segment being measured and the least upper bound of S.

Case 2. The measuring process may produce an infinite set T of rational numbers approximating the length of a line segment. It may happen that

(1) There is a rational measure for the given segment.

(2) There is a rational least upper bound of T.

Let us consider a line segment $\overline{EF}$ whose length we know is $\frac{1}{3}$ centimeter. If we follow the measuring process, with a unit u of length 1 centimeter, we get the following set of rational numbers approximating the length of $\overline{EF}$.

$$T = \{0, 0.3, 0.33, 0.333, 0.3333, \ldots\}.$$

You may want to check the first few approximations yourself. From your study of rational numbers you can deduce that $\frac{1}{3}$ is the l.u.b. of T.

In this case we knew the centimeter measure of a line segment to be $\frac{1}{3}$ even before we applied the measuring process to the segment. We considered the infinite set T of rational numbers produced by the measuring process and found that $\frac{1}{3}$ is the least upper bound of T.

Case 3. The measuring process produces an infinite set of rational numbers approximating the measure of a line segment. It may happen that there is no rational number which represents the least upper bound of the set.

Re-examine the problem of calculating length of a diagonal in a square, the question posed in Section 5.3 which initially led to a study of the measuring process. Instead of considering just the case of a square whose sides have length 1 centimeter, let us look at the side of any square and at one of its two congruent diagonals (see Figure 5.5). Suppose it were possible to find a common unit of measurement for the side and the diagonal, whether it be a segment of length 1 centimeter or 1 inch or of any other length. Then, the length of the side of the square could be expressed as an integral number of these units, say x units, and the length of the diagonal as y units.

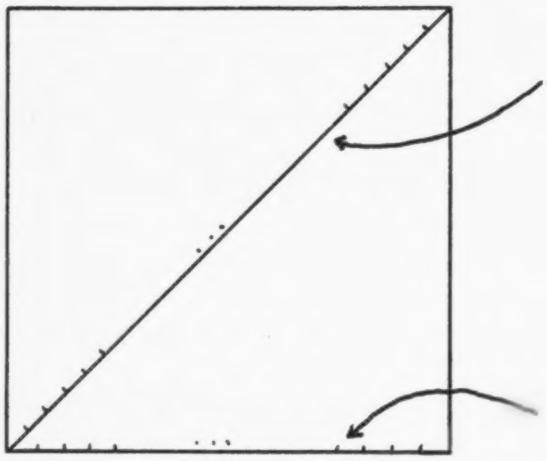

y segments, each congruent to a unit u
x segments, each congruent to a unit u

Figure 5.5

By the Pythagorean property, we know that

$$x^2 + x^2 = y^2$$
$$2x^2 = y^2.$$

But, earlier in this chapter, we saw that for any positive integers x and y, $2x^2 \neq y^2$. This means that regardless of the unit used for measuring, it is impossible to express both the length of a side and the length of a diagonal of a square in terms of this unit. Thus we cannot express the ratio of the length of the diagonal to the length of the side as a rational number.

Now, consider a square with sides 1 centimeter long. The measuring process produces the following set of rational numbers approximating the length of the diagonal.

$$A = \{1, 1.4, 1.41, 1.414, 1.4142, ---\}$$

The exact length of this diagonal cannot be expressed by a rational number. More specifically, the centimeter length of the diagonal is a number whose square is 2 and we have shown that there is no such number in Q. Definition 3 states that the length of this diagonal is the least upper bound of set A. But, while set A has many upper bounds in Q such as 2, $4\frac{1}{2}$, and 7, there is no number in Q which is the least upper bound of A. Set A is a non-empty set of rational numbers which is bounded from above but which has no least upper bound.

In Section 5.9, we will begin to see what can be done to remedy this situation.

5.8 Exercises

1. Find the least upper bound in Q of each of the following sets (assume that the pattern in (d) continues).

   (a) $\{.3\}$ (c) $\{.3, .33, .333\}$

   (b) $\{.3, .33\}$ (d) $\{.3, .33, .333, .3333, \ldots\}$.

2 Find all integers x which satisfy the following inequations.

   (a) $0 < \frac{x}{10} < \frac{2}{3}$ (c) $0 < \frac{x}{100} < \frac{1}{15}$

   (b) $0 < \frac{x}{100} < \frac{2}{3}$ (d) $0 < \frac{x}{1000} < \frac{1}{150}$

3. Suppose you began with a segment $\overline{CD}$ whose length is $\frac{2}{3}$ centimeters. Without doing any measuring, list the first 3 approximations to the length of $\overline{CD}$ that would be produced by the measuring process.

4. Suppose the measuring process, when applied to a particular line segment, does end. What can you say about the length of the segment? Support your answer.

5. Express each of the following rational numbers as a decimal fraction.

(a) $\frac{3}{5}$ (b) $\frac{1}{7}$ (c) $\frac{2}{9}$ (d) $\frac{475}{1000}$ (e) $\frac{1}{8}$

5.9 The Real Number System

In each of the three situations studied in Section 5.7, the length of a line segment was being measured. The measuring process was always the same, but the sets of rational numbers were quite different. We examined two aspects of each situation:

(1) The set of rational numbers involved

(2) The least upper bound of this set (length of the segment)

We were guided throughout our examination by Definition 3 which states that the length of a given line segment is the least upper bound of the set of rational numbers generated by the measuring process. However, we observed that for one of the three line segments, there is no rational number which is the least upper bound of the corresponding set of approximations. Thus, the ordered field $(Q,+,\cdot,<)$ is inadequate to express accurately the length of every line segment we encounter. In other words, it is possible for us to have a non-empty set of rational numbers which is bounded from above but has no least upper bound in $(Q,+,\cdot,<)$.

Overcoming this difficulty requires another extension of the number system--this time from the rational numbers to a new ordered field $(R,+,\cdot,<)$ called the real number system. The real numbers contain the rational numbers as a subfield and new elements to serve as least upper bounds for trouble-some sets of rationals arising from the measuring process.

There would be little virtue in creating a new system to supply least upper bounds for sets of rationals if the new system produced new sets of numbers without least upper bounds. Therefore, in the real number system every non-empty subset of R that is bounded from above has a least upper bound in R. For this reason, the ordered field $(R,+,\cdot,<)$ is called complete.

What kind of new objects are introduced by this extension of Q to R? How are the new numbers to be named? What rules govern operations and order in $(R,+,\cdot,<)$?

Let us turn our attention to the names of the real numbers in R. First of all, remember that $Q \subset R$; every rational number is a real number. We have already seen that some rational numbers can be expressed by a terminating decimal fraction while others have decimal fraction representations that are infinite and repeating. For example,

$$\frac{1}{2} = .5$$

$$\frac{2}{5} = .4$$

$$\frac{1}{8} = .125$$

$$\frac{1}{3} = .333\overline{3}$$

$$\frac{8}{33} = .24242\overline{4}$$

Each rational number, whether it is named by an infinite, repeating decimal fraction or by a terminating decimal fraction, is an element in R. Thus, .4, .325, $.018018\overline{018}$, and $.666\overline{6}$ are all elements in R. The bar "-" indicates the digits which repeat. For example:

$.\overline{3} = .333\overline{3} = .3333\overline{3}$, and $.\overline{24} = .24\overline{24} = .2424\overline{24}$, etc.

We already know that R contains other real numbers which are not in Q, that is, real numbers which are not rational numbers. These real numbers are called irrational numbers. For example, we saw that when measuring a diagonal of a square whose side has length 1 centimeter, the measuring process produced the following set of rational numbers:

$$T = \{1, 1.4, 1.41, 1.414, \ldots\}.$$

We saw that there was no rational number which is the least upper bound of T. If we denote this least upper bound by "ℓ" then we know $\ell \in R$, and that ℓ is an irrational number. However, we would like to be able to name this least upper bound more explicitly than by calling it "ℓ", perhaps in such a way that the name would remind us of the elements of T. Since we have listed only 4 elements in T, we are restricted to these few rational numbers in naming ℓ. We write "$\ell = 1.414\ldots$" The dots, as usual, indicate that the digits in this decimal representation continue indefinitely, just as the set T contains infinitely many elements. The fact that no bar "-" appears indicates that no block of digits continues to repeat indefinitely. Unfortunately the name "1.414..." for ℓ does not indicate any pattern which might be used to determine the next digit in the decimal. If the list of elements in T contained another approximation to the length of the diagonal, then we would have

$$T = \{1, 1.4, 1.41, 1.414, 1.4142, \ldots\}$$

and we would be able to name the least upper bound ℓ by "1.4142..." Thus, the name used for the least upper bound of T depends upon the number of elements in the set actually listed. In practice, if you wanted to use ℓ in a problem involving computations, you would "round off" this infinite decimal to a finite number of places, depending upon the accuracy desired. 1.4142, for example, would be considered a more accurate approximation to ℓ than 1.414. The more accuracy needed, the greater the number of approximations in T that must be considered. We will name ℓ another way in Section 5.11.

It appears that each real number can be named by a decimal representation in one of the following forms:

(1) A terminating decimal such as .5 or 2.7518.

(2) An infinite, repeating decimal such as $.7171\overline{71}$ or $.1838\overline{83}$.

(3) An infinite decimal which does not repeat such as .812574916638.... (Since there is no bar "-" we cannot establish a pattern that will enable us to state the next digit in this infinite decimal)

Since we could take any terminating decimal such as .7518 which is listed above, and write it as the infinite decimal $.7518000\overline{0}$ where the zeros continue indefinitely to the right, we are really able to view every decimal representation as an infinite decimal. You will see, as you gain experience working with real numbers, that some real numbers will have two different decimal representations; that is, there will be two infinite decimal names for the same real number. For example,

"$1.000\overline{0}$" and "$.99999\overline{9}$" both name the same real number, likewise "$.4130000\overline{0}$" and "$.412999\overline{9}$" both name the same real number.

5.10 Exercises

1. For each of the following properties, tell whether the property is true of W, Z, Q or R. A given property may be true for more than one of these sets.
   (a) For each positive element a in the set, there is a positive integer N so that $N > a$.
   (b) Every element in the set may be written as $\frac{p}{q}$ where p, q are integers and $q \neq 0$.
   (c) Every non-empty subset which is bounded from above has a ℓ.u.b.
   (d) Every element in the set has an infinite decimal representation.
2. In each case, tell whether x represents a rational number, an irrational number or neither.
   (a) $x \in R$ and $x^2 = 2$. (d) $x = 0$
   (b) $x = .9817$ (e) $x = .66\overline{66}$
   (c) $x \in Q$ and $x^2 = 2$. (f) $x = y + 3$ where $y \in R$ and $y^2 = 2$.
3. Prove that if a is an irrational number and b is a rational number but $b \neq 0$, then $a \cdot b$ is an irrational number.
4. Give an example to show that the product of two irrational numbers may be rational.
5. Prove that if x and y are both rational numbers, then $x \cdot y$ is a rational number.
6. For each of the following pairs of infinite decimals, tell

which represents the greater real number.

(a) $.4139;\ .407481$ (c) $.4;\ .400\overline{0}$ (e) $1.00\overline{0};\ .99\overline{9}$

(b) $.33\overline{3};\ .338488\overline{8}$ (d) $0.3614;\ .3644\overline{4}$

7. In which of the following decimals do you know the digits that follow?

(a) $.4747\overline{47}$ (d) $2.343\ldots$

(b) $8.37474\ldots$ (e) $.7575\overline{75}$

(c) $.1233\overline{3}$ (f) $.333\cdots$

5.11 Some Properties of the Real Number System

Ordering of the Real Numbers

One way to order a pair of rational numbers is by inspecting their corresponding decimal fraction representations. Remember that

$$8.3 < 8.4,\ .2563 < .2567$$

and, in general, for two terminating decimal fractions

$$.a_1a_2a_3a_4 \text{ and } .b_1b_2b_3b_4,$$

you look for the first place (reading from left to right) in which they disagree; the one which has the smaller entry in that place represents the smaller number. This same procedure may be used to compare any two decimals, infinite or terminating.

Example 1. Which is smaller, $.7183946\cdots$ or $.7184623\cdots$? Notice that the first three digits of these infinite decimals agree place by place. The fourth decimal place is the first one in which they differ and $3 < 4$.

Therefore, $.7183946\ldots < .7184623\ldots$

Example 2. Which is smaller, .8163 or .8163419...? The first decimal, though terminating, may be written as $.816300\overline{0}$. If we compare "$.816300\overline{0}$" and ".8163419..." we find that the fifth decimal place is the first one in which they differ. Since $0 < 4$, we conclude that

$$.8163 < .8163419.$$

We mentioned, in Section 5.9, that certain real numbers have two different infinite decimal representations. For these numbers we will have to modify the above mentioned procedure.

Example 3. We know that $1.0000\overline{0} = 0.9999\overline{9}$. Yet, if you follow the procedure for comparing infinite decimal representations, you will conclude erroneously that $0.9999\overline{9} < 1.0000\overline{0}$.

Example 4. We know that

$$.2300\overline{0} = .22999\overline{9}.$$

Again, if you compare these decimals, place by place, you will conclude erroneously that

$$.22999\overline{9} < .23000\overline{0}.$$

When the bar is above a zero there are two distinct decimal representations for the same real number. In all other cases if

$$x = .a_1a_2a_3a_4\cdots \text{ and}$$

$$y = .b_1b_2b_3b_4\cdots,$$

you can decide which of the two decimals represents the smaller real number by looking for the first place (reading from left to right) in which they disagree; the one which has the smaller entry in that place represents the smaller number.

The equation "$x^n = a$" in $(R,+,\cdot,<)$

Suppose that we are interested in the solution of the equation $x^2 = 3$. We know that the solution set $A = \{x\colon x \in Q \text{ and } x^2 = 3\}$ is empty. (See Section 5.2, Exercise 2.) Let us examine the solution set $B = \{x\colon x \in R \text{ and } x^2 = 3\}$. Consider the following approximations to an element x in B. Since $1^2 = 1$ and $2^2 = 4$, we see that $1 < x < 2$. Let us take 1 as a first approximation to x. Since $(1.7)^2 = 2.89$ while $(1.8)^2 = 3.24$;

$$1.7 < x < 1.8.$$

Take 1.7 as a second approximation to x. If we continue this procedure, we generate the following set of approximations to x:

$$C = \{1, 1.7, 1.73, 1.732, 1.7320, \cdots\}.$$

We see that set C is non-empty and is bounded from above. (Verify this statement.) By the completeness property of R, we may say that the least upper bound ℓ of C is in R. Using the five approximations in C, we may name ℓ as "1.7320···" Notice again, that we cannot predict the next digit in "1.7320···" without calculating another approximation in C. Since $\ell^2 = 3$ and $\ell > 0$, ℓ is called the positive square root of 3 and is written "$\ell = \sqrt{3}$." Thus, $\sqrt{3} \in R$. In the same way, we write $x = \sqrt{5}$ if and only if $x > 0$ and $x^2 = 5$. In general, if a and b are real numbers and $a, b > 0$, then b is a positive square root of a, written $b = \sqrt{a}$, if and only if $b^2 = a$. The ℓ of Section 5.9 can be renamed, $\ell = \sqrt{2}$. Also, $b = \sqrt{7}$ if and only if $b > 0$ and $b^2 = 7$ and $b = \sqrt{\frac{3}{5}}$ if and only if $b > 0$ and $b^2 = \frac{3}{5}$. Notice that if $x = -\sqrt{7}$, then $x^2 = 7$; x is called the negative square root of 7. For every positive square root of a number, there is also a negative square root which is the additive inverse of the positive square root.

Each square root of a number mentioned above is in R. If a is a positive real number, then the positive square root of a (written "$\sqrt{a}$") and the negative square root of a (written "$-\sqrt{a}$") are in R.

In fact, if n is a positive integer and if a is a positive real number, the equation $x^n = a$ has a unique positive solution in R. This solution is written "$x = \sqrt[n]{a}$" or "$x = a^{1/n}$." For example, the solution to the equation $x^3 = 4$, $x = \sqrt[3]{4}$, is in R; the solution to the equation $x^7 = 10$, $x = \sqrt[7]{10}$, is in R.

The Archimedean Property of $(R,+,\cdot,<)$

Example 5. Is there a positive integer greater than the real number 7.813942...? It is easy to answer this question simply by naming one positive integer, say 8, which is greater than 7.813942...

Example 6. Is there a positive integer greater than the real number $128.1717\overline{17}$? Again, we simply name the integer 129, which is greater than $128.1717\overline{17}$.

Example 7. Is there a positive integer greater than the real number $\sqrt{3}$? Since $1^2 = 1$ and $2^2 = 4$ we know that $1 < \sqrt{3} < 2$. In fact we have seen that $\sqrt{3} = 1.7320...$ Thus $2 > \sqrt{3}$.

Now let us state this idea in a more general form.

(1) Given any positive real number a, there is a positive integer N such that $N > a$.

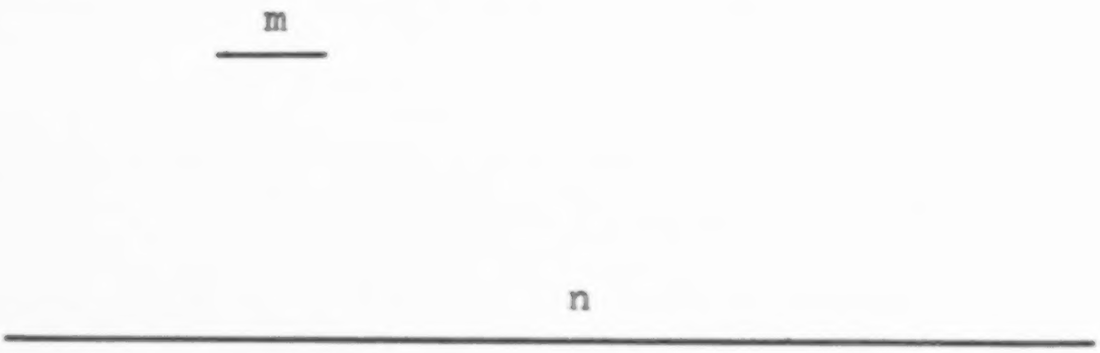
This statement is called the Archimedean Property of the complete ordered field $(R,+,\cdot,<)$; consequently, the system of real numbers is sometimes referred to as a complete Archimedean ordered field. (Archimedes himself attributed this "Archimedean Property" to Eudoxus, a contemporary of Plato (c. 350 B.C.).)

Sometimes the Archimedean property is stated in an apparently different form. Before we state it, consider the following problem.

Draw any two line segments. Let "m" represent the length of one segment and "n" the length of the other. (See Figure 5.4(a).) We know that $m \in R$ and $n \in R$. (Why?) Do you think it is possible to lay off a string of congruent segments, say N segments, each having length m so that the total length of the segments is greater than n?

If we lay off a string of 11 congruent segments each having length m, we get a segment $\overline{XY}$ whose length is greater than n. (See Figure 5.4(b).)

An alternate form of the Archimedean property guarantees that given segments of lengths m and n, we can always put together some number of congruent segments, each of length m, to construct a segment of length greater than n. This is stated more succinctly as:



(a)

Comparison of segments of length m and length n

m m m m m m m m m m m
X
Y

(b)

11 congruent segments each of length m

Figure 5.6

(2) If m and n are positive real numbers, there is a positive integer K such that $Km > n$.

Actually, statements (1) and (2) are equivalent; that is, each one implies the other. (See Section 5.12, Exercises 9 and 10.) The following examples also serve to illustrate this alternate form of the Archimedean property:

Example 8. Given $a = \frac{5}{2}$ and $b = 17$, is there a positive integer N such that $N \cdot \frac{5}{2} > 17$? If $N = 7$, then $7 \cdot \frac{5}{2} > 17$.

Example 9. Given $a = \sqrt{2}$ and $b = 20$, is there a positive integer N such that $N \cdot \sqrt{2} > 20$? Take $N = 20$. Since $\sqrt{2} > 1$, $20\sqrt{2} > 20 \cdot 1$. Thus $20 \cdot \sqrt{2} > 20$.

5.12 Exercises

1. List the following decimals in ascending order.
    - (a) 3.1847
    - (b) $3.199\overline{9}$
    - (c) 3.201
    - (d) $3.022\overline{2}$
2. Find five approximations to $\sqrt{5}$. How is the set of approximations used to name $\sqrt{5}$ by an infinite decimal?
3. Which of the following represent rational numbers?
    - (a) $.74321...$
    - (b) $\sqrt{13}$
    - (c) $\sqrt{2} + \sqrt{3}$
    - (d) $\sqrt{1.21}$
    - (e) 0
4. Prove that $4 + 3\sqrt{2}$ is irrational.
5. For each of the following real numbers, find a positive integer N such that $N > x$:

(a) $\sqrt{13}$ (b) $\sqrt{2} + \sqrt{7}$ (c) $6\frac{1}{3}$ (d) .4999 (e) $(\sqrt{11})^2$

6. Indicate how the least upper bound of each of the following sets is named:

   (a) $\{1, 1.4, 1.41, 1.414, 1.4142, \ldots\}$

   (b) $\{0, 0.3, 0.33, 0.333, \ldots\}$

   (c) $\{3, 3.1, 3.14, 3.141, 3.1415, \ldots\}$

   (d) $\{6, 6.1, 6.16, 6.161, 6.1616, \ldots\}$

   (e) $\{1, 1.78, 1.783\}$

   (f) $\emptyset$

7. Find the following square roots:

   (a) $\sqrt{9}$ (c) $\sqrt{25}$ (e) $\sqrt{36}$ (g) $\sqrt{\frac{81}{49}}$

   (b) $\sqrt{4}$ (d) $\sqrt{\frac{9}{4}}$ (f) $\sqrt{\frac{1}{121}}$ (h) $\sqrt{0}$

8. Find the following square roots:

   (a) $\sqrt{4 \cdot 9}$ (c) $\sqrt{81 \cdot 36}$ (e) $\sqrt{0 \cdot 16}$ (g) $\sqrt{\frac{100}{25}}$

   (b) $\sqrt{16 \cdot 4}$ (d) $\sqrt{121 \cdot 64}$ (f) $\sqrt{1 \cdot 25}$ (h) $\sqrt{\frac{64}{4}}$

9. Assume that if x is a positive rational number, you can always find a positive integer N such that $N > x$. Prove that if a and b are positive rational numbers, there is a positive integer N such that $Na > b$. (Hint: Consider $\frac{b}{a}$.)

10. Assume that if a and b are positive rational numbers, there is a positive integer N such that $Na > b$. Prove that if x is a positive rational number, there is a positive integer N such that $N > x$. (Hint: Take $a = 1$.)

5.13 Arithmetic of Irrational Numbers

In any field, equations of the type $ax + b = c$ $(a \neq 0)$ have unique solutions given by the expression $\frac{c - b}{a}$. For example, the equation $3x + 12 = -18$ has solution

$$\frac{-18 - 12}{3} = -10 \qquad (1)$$

in $(Q,+,\cdot)$. The equation $(5\sqrt{6})x + 4\sqrt{12} = 7\sqrt{12}$ has solution

$$\frac{7\sqrt{12} - 4\sqrt{12}}{5\sqrt{6}} \qquad (2)$$

in $(R,+,\cdot)$. The expression giving the solution in (1) was easily simplified by application of arithmetic facts. But any comparable simplification in (2) depends on knowledge of arithmetic facts and rules involving irrational numbers.

In any field $(F,+,\cdot)$, the distributive property of multiplication over addition implies

$$ax + b\cdot x = (a + b)\cdot x.$$

Therefore, in the real number field,

$$\begin{aligned} 7\sqrt{12} - 4\sqrt{12} &= 7\sqrt{12} + (-4)\sqrt{12} \\ &= (7 + (-4)\sqrt{12} \\ &= 3\sqrt{12}. \end{aligned}$$

And, in general

For all a, b, c in R, if $b > 0$,
then $a\sqrt{b} + c\sqrt{b} = (a + c)\sqrt{b}$.

This rule for calculating with irrational numbers permits simplifications like

$$17\sqrt{6} - 4\sqrt{6} = 13\sqrt{6},$$

$$\frac{4}{3}\sqrt{5} + 2\sqrt{5} = \frac{10}{3}\sqrt{5},$$

$$-12\sqrt{3} + \frac{17}{2}\sqrt{3} = -\frac{7}{2}\sqrt{3}, \text{ etc.}$$

The following computations suggest another arithmetic rule useful in simplifying expressions with irrational components.

$$\sqrt{9}\sqrt{4} = 3 \cdot 2 = 6 = \sqrt{36} = \sqrt{9 \cdot 4}$$

$$\sqrt{9}\sqrt{\frac{4}{9}} = 3 \cdot \frac{2}{3} = 2 = \sqrt{4} = \sqrt{9 \cdot \frac{4}{9}}$$

$$\sqrt{16}\sqrt{36} = 4 \cdot 6 = 24 = \sqrt{576} = \sqrt{16 \cdot 36}.$$

The rule suggested by these examples is $\sqrt{a}\sqrt{b} = \sqrt{ab}$. But, in each example, a and b were perfect squares of rational numbers. Does the rule hold for $\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{6}$?

(1) $\sqrt{2}\sqrt{3} = \sqrt{6}$ if and only if

$(\sqrt{2} \cdot \sqrt{3})^2 = (\sqrt{6})^2 = 6.$

(2) But $(\sqrt{2} \cdot \sqrt{3})^2 = (\sqrt{2}\sqrt{3})(\sqrt{2}\sqrt{3})$ (Why?)

$= (\sqrt{2}\sqrt{2})(\sqrt{3}\sqrt{3})$ (Why?)

$= 2 \cdot 3$ (Why?)

$= 6.$

A similar argument can be used to prove

For all a,b in R, if $a \geq 0$ and $b \geq 0$

then $\sqrt{a}\sqrt{b} = \sqrt{ab}$.

This rule for calculating with irrational numbers permits simplifications like

$$\frac{5\sqrt{8}}{\sqrt{2}} = \frac{5\sqrt{4}\sqrt{2}}{\sqrt{2}} = 10,$$

$$\frac{3\sqrt{12}}{5\sqrt{6}} = \frac{3\sqrt{2}\sqrt{6}}{5\sqrt{6}} = \frac{3}{5}\sqrt{2},$$

$$\sqrt{8x^3y^2} = \sqrt{4}\sqrt{2}\sqrt{x^2}\sqrt{x}\sqrt{y^2}$$

$$= 2xy\sqrt{2x}, \text{ etc.}$$

Another enticing conjecture about rules for manipulating radicals is $\sqrt{a} + \sqrt{b} = \sqrt{a + b}$. But be careful! Complete the following computations to check this tentative rule.

$$\sqrt{4} + \sqrt{9} = 2 + 3 \neq \sqrt{13}$$

$$\sqrt{25} + \sqrt{36} = 5 + 6 \neq \sqrt{51}$$

$$\sqrt{15} + \sqrt{1} \neq \sqrt{16} \quad \text{since} \quad \sqrt{1} = 1 \text{ and } \sqrt{15} > 3.$$

As you can see, $\sqrt{a} + \sqrt{b} \neq \sqrt{a + b}$ for most real numbers a and b.

Question. Check some specific cases of these conjectures:

$$\sqrt{a - b} = \sqrt{a} - \sqrt{b}? \qquad \sqrt{\frac{a}{b}} = \frac{\sqrt{a}}{\sqrt{b}}?$$

These rules for manipulating radicals permit simplification of expressions and solution of equations in $(R,+,\cdot)$.

5.14 Exercises

1. Simplify the following radical expressions:

   (a) $\sqrt{45}$ (= $3\sqrt{5}$)

   (b) $\sqrt{24}$

   (c) $\sqrt{12x^3}$

   (d) $\sqrt{96}$

   (e) $\sqrt{\frac{100x^2}{9}}$

   (e) $\sqrt{x^2 - 2x + 1}$

   (f) $\sqrt{28x^3y^2}$

   (g) $\sqrt{8}$

   (h) $\sqrt{32}$

   (i) $\sqrt{\frac{16}{25}x^3}$

2. Write each of these expressions in equivalent radical form.

   (a) $2\sqrt{3}$ (= $\sqrt{4}\sqrt{3} = \sqrt{12}$)

   (b) $7\sqrt{9}$

   (c) $3x\sqrt{2}$

   (d) $5\sqrt{13}\sqrt{4}$

   (e) $2xy\sqrt{5}$

   (f) $3x^2\sqrt{y}$

   (g) $5a^2b^3$

Solve each of the following equations in $(R,+,\cdot)$.

3. $7\sqrt{3}x + 8 = 14$
4. $5x - 3\sqrt{2}x = 12\sqrt{2}$
5. $x^2 - 5x = 14$
6. $4x^2 - 9 = 0$
7. $x^2 - 12 = 0$
8. $3x^2 - 17 = 12$
9. $x^2 + 9x + 20 = 0$
10. $4x^2 + 7x - 12 = 3x^2 + 15 + x$
11. $\sqrt{3x^2} = \sqrt{6} + 5$
12. $\sqrt{x^2 - 12x + 32} = 0$

Prove.

*13. If a,b are real numbers greater than or equal to 0,

$$\sqrt{\frac{a}{b}} = \frac{\sqrt{a}}{\sqrt{b}}$$

14. $\sqrt{a} - \sqrt{b} \neq \sqrt{a - b}$ for some a,b in R.

*15. If a,b are real numbers greater than or equal to 0,

$$\sqrt{ab} = \sqrt{a}\sqrt{b}.$$

5.15 Summary

In this chapter we introduced the real number system $(R,+,\cdot,<)$. This system is an ordered field which contains the ordered field of rational numbers as a subset. An essential difference between the two systems is the completeness property of $(R,+,\cdot,<)$.

1. The ordered field $(Q,+,\cdot,<)$ is inadequate to answer certain mathematical problems we encounter. In particular:

   (a) The equation $x^2 = 2$ has an empty solution set in

$(Q,+,\cdot,<)$.

(b) There is no number in Q which expresses the length of a diagonal of a square whose side has a length of one unit.

2. An examination of the process we use to measure the length of a line segment indicated that a set of rational numbers is produced. If the process ends, the set is finite and includes the length of the segment. If the process does not end, then each rational number is an approximation to the length of the segment. We saw that, in all cases, the length of the segment being measured could be defined as follows:

   > The length of a line segment is the *least upper bound* of the set of rational numbers which arises from the measuring process.

3. We considered several cases in which the measuring process was applied to various line segments and observed that there was not always a rational number to measure each length. Thus, certain sets of rational numbers produced by the measuring process do not have a least upper bound in $(Q,+,\cdot,<)$.

4. To overcome this difficulty we introduced a new ordered field $(R,+,\cdot,<)$ in which every set of rational numbers arising from the measuring process would have a least upper bound. Thus, in this new ordered field, we can measure the length of every line segment. Since some line segments have rational numbers as measures, $Q \subset R$.

5. The elements of R are called real numbers. Since $Q \subset R$, some real numbers are also rational numbers. Those real numbers which are not rational numbers are called irrational numbers.
6. $(R,+,\cdot,<)$ has the Archimedean Property.
7. If n is a positive integer and if a is a positive real number, the equation $x^n = a$ has a unique positive solution in R.

5.16 Review Exercises

1. Let n be a natural number which contains 6 factors of 2 in its complete factorization into primes. For each of the following numbers, determine the number of factors of 2 in its complete factorization into primes.

   (a) $2n$ (b) n^2 (c) $\frac{n}{2}$ (d) n^3
2. Prove that $7\sqrt{2}$ is not a rational number. (Hint: Assume there are integers p and q, $q \neq 0$, so that $\frac{p}{q} = 7\sqrt{2}$.)
3. Prove that the solution set $\{x: x \in Q \text{ and } x^2 = 17\}$ is empty.
4. What does it mean to say that $(Q,+,\cdot)$ is inadequate to solve an equation?
5. Find the length of a diagonal of a square whose side has a length of:

   (a) 2 cm. (b) 5 cm. (c) $\sqrt{2}$ cm. (d) a cm.
6. Let "d" represent the centimeter length of a diagonal of a square whose sides have length 1 cm. How many congruent segments each having a length of d centimeters, would you

have to use if you wanted to form a segment whose length would be greater than 10 centimeters?

7. Find four approximations to $\sqrt{7}$. For example Since $2^2 < 7$ but $3^2 > 7$, 2 is the first approximation.

8. Find the least upper bound in $(Q,+,\cdot,<)$ [if there is one] of each of the following sets: (assume that the pattern continues in parts (a) and (b))

(a) $\{1, 2, 3, 4, 5, \ldots\}$ (c) $\{7, 7.1, 7.13, 7.138\}$

(b) $\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \ldots\}$ (d) $\{x: x \in Q \text{ and } x^2 < 7\}$.

9. (a) Find an upper bound for $\emptyset$ in $(Q,+,\cdot,<)$; in $(R,+,\cdot,<)$.

(b) Find the least upper bound of $\emptyset$ in $(Q,+,\cdot,<)$; in $(R,+,\cdot,<)$.

10. Now that you have worked with the definition of an upper bound and the least upper bound of a set S in an ordered field $(F,+,\cdot,<)$, suggest a definition for:

(a) x is a lower bound of S.

(b) x is the greatest lower bound of S.

11. Suppose the measuring process produced the following infinite set of rational numbers: $S = \{0, .1, .11, .111, .1111, \ldots\}$ where the indicated pattern is assumed to continue indefinitely.

(a) What is the next approximation in S?

(b) Is there a greatest rational number in S?

(c) Give an upper bound of X.

(d) What would you guess is the least upper bound of S?

12. For each of the following equations, represent its positive real number solution:

(a) $x^2 = 13$ (b) $x^3 = 8$ (c) $x^5 = 25$ (d) $x^5 = 32$

13. Which of the solutions in Exercise 11 are rational?
14. Explain why the least upper bound of a finite set of rational must be a rational numbers.

CHAPTER 6

COORDINATE GEOMETRY

6.1 Introduction

You saw in Chapter 3 (Section 3.6) that if we replace "point" with "commando," "line" with "team," and "plane P" with "the commando squad" we obtain a system that satisfies the incidence axioms. In fact, you saw that there are other meanings for lines and points which also result in models that satisfy those axioms. It is therefore clear that those axioms are not sufficient by themselves to characterize points and lines as we ordinarily think of them. In this chapter we add three more axioms to our list of axioms. This increased collection of axioms will indeed characterize the lines and points of our experience, and some of the models which satisfied the incidence axioms will not satisfy the six axioms. We are going to be guided in our choice of the additional axioms by our experiences with rulers and with our enlargement of the rational number system to the real number system.

This does not mean that we are making obsolete the theorems we proved in Chapter 3. In fact, they are still in force and are available in our continuing study of geometry in this chapter.

We repeat the incidence axioms here for convenient reference. Recall that π was the name of the plane.

Axiom 1. (a) Plane π is a set of points, and it contains at least two lines.

(b) Each line in plane π is a set of points, containing at least two points.

Axiom 2. For every two points in plane π there is one and only one line in π containing them.

Axiom 3. For every line m and point E in the plane π, there is one and only one line in π containing E and parallel to m.

6.2 Axiom 4. Uniqueness of Line Coordinate Systems

As we said, our experiences with rulers suggest this axiom.

Suppose you wish to draw a ruler on a line. You start with an unmarked line, as in Figure 6.1,

Figure 6.1

assuming it to be endless. Then you choose any two points, call one 0 and the other I. Perhaps the line then looks like Figure 6.2,

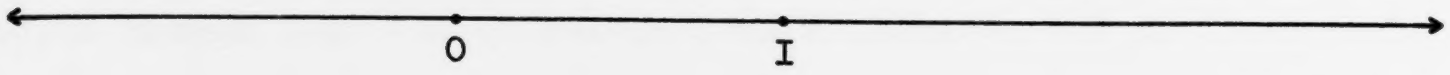


Figure 6.2

or perhaps like Figure 6.3.

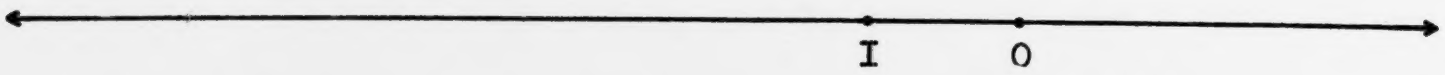


Figure 6.3

Then you assign 0 (zero) to 0 and 1 to I. Having done this you will have no other choices in assigning all other real numbers to points of the line. For the ruler in Figure 6.2 some of the assignments are shown in Figure 6.4.

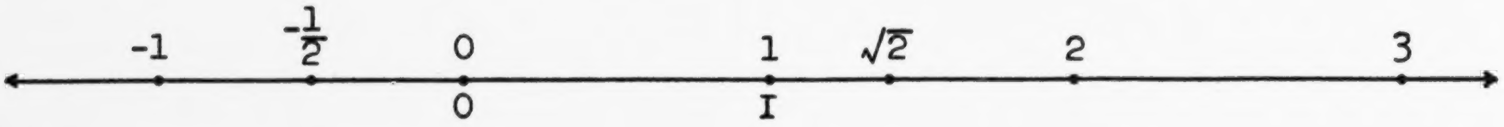


Figure 6.4

For the ruler in Figure 6.3 these assignments are shown in Figure 6.5.

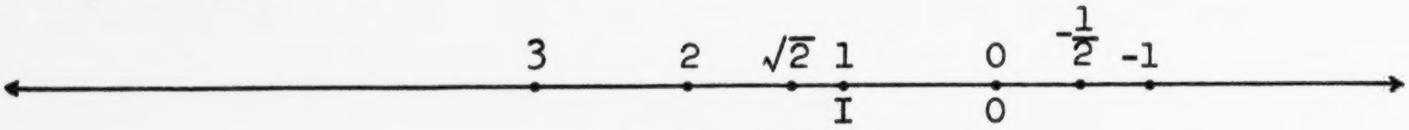


Figure 6.5

In assigning a different number to each point we are actually assuming that there are as many points on a line as there are real numbers. Only under this assumption can we set up a one-to-one correspondence between the set of points on a line and the set of real numbers. Recall that Axiom 1(b) tells us that each line contains at least two points. Axiom 4 adds information about the number of points on a line. But it does more than that. It says also that once you have chosen the two points to which are assigned 0 and 1, there is exactly one way to make all other assignments of numbers to points, in order to get the one-to-one correspondence in which we are interested. Of course there are many one-to-one correspondences between a line and a set of real numbers, even after O and I have been chosen. In Figure 6.6 we indicate some of these one-to-one correspondences,

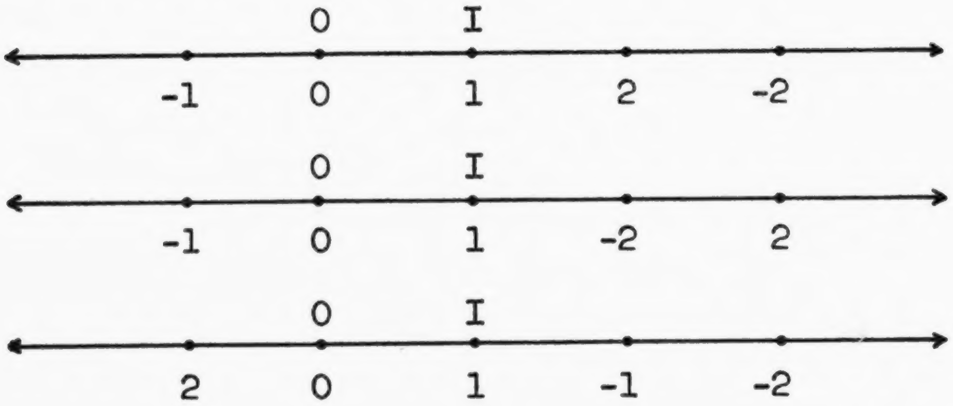


Figure 6.6

but not all of them are acceptable. Let us call the acceptable one-to-one correspondences coordinate systems on a line. We are now ready to state Axiom 4 precisely.

Axiom 4. For each pair of distinct points A and B of a line there is exactly one coordinate system on that line in which A corresponds to 0 and B corresponds to 1.

The line coordinate system described in Axiom 4 is called the A,B-coordinate system on the line, taking its name from the ordered pair of points (A,B), called the base. A and B are called the base points. The point A that corresponds to zero is called the origin and the point B that corresponds to one is called the unit-point. The number assigned to a point of $\overleftrightarrow{AB}$ is called its A,B-coordinate.

These terms are illustrated in Figure 6.7. Note that there are two coordinate systems indicated on one line. (A,B) is the base of one. What is the base of the other?

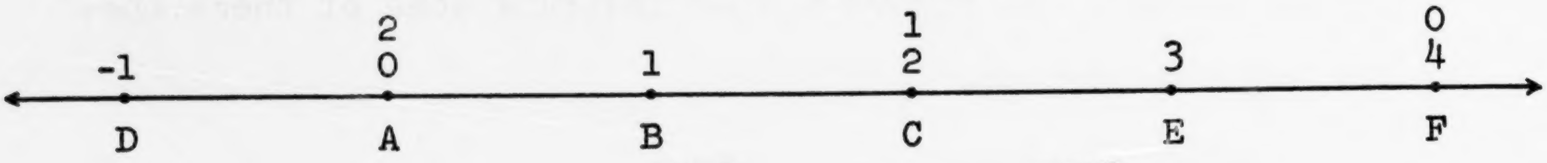


Figure 6.7

In the A,B-coordinate system the origin is A, the unit-point is B and the A,B-coordinate of C is 2. In the F,C-coordinate system, the origin is F, the unit point is C and the F,C-coordinate of A is 2.

Definition. Let line ℓ have an A,B-coordinate system and let P and Q be any two points of ℓ. Suppose their A,B-coordinates are p and q respectively. Then the number given by $|p - q|$ is called the A,B-distance between P and Q.

Examples. In Figure 6.7 the A,B-distance between C and E is $|2 - 3| = 1 = |3 - 2|$ which is the A,B-distance between E and C.

Theorem 1. (a) The A,B-distance between A and B is 1.

(b) The A,B-distance between P and Q is equal to the A,B-distance between Q and P.

(c) The A,B-distance between P and Q is equal to 0 if and only if P = Q.

Proof. Exercise.

6.3 Exercises

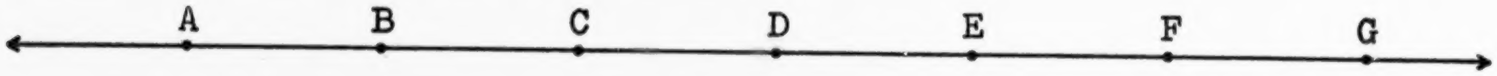
In these exercises assume that all line coordinate systems look like the number lines you have been using.

1. Assume an O,I-coordinate system. What is its origin? What is its unit-point? What do you think is the O,I-coordinate of the midpoint of $\overline{OI}$?

2. (a) Draw a horizontal line; on it choose two points $\frac{1}{2}$ inch apart; call one A, the other B. Locate the points whose A,B-coordinates you think are -1, 2, $3\frac{1}{2}$, $-2\frac{1}{3}$, $\sqrt{3}$.

   (b) Draw another line below $\overleftrightarrow{AB}$, and name the points below A and B, C and D respectively. On this line locate the points whose D,C-coordinates you think are -1, 2 $3\frac{1}{2}$, $-2\frac{1}{3}$, $\sqrt{3}$.

3. In this exercise use the diagram below, assuming that the points named are evenly spaced.



   (a) What is the C,D-coordinate of E? of B?

   (b) What is the D,C-coordinate of E? of B?

   (c) What is the B,D-coordinate of F? of G?

   (d) What is the G,D-coordinate of A? of E?

   (e) What is the A,G-coordinate of B? of E?

4. Tell whether each of the following statements is true or false. In each, A,B, and C are names of distinct points on a line ℓ.

   (a) There is exactly one coordinate system on ℓ that has A as origin.

   (b) For each choice of a point X on ℓ, other than A, there is a different A,X-coordinate system.

   (c) For each choice of a point Y on ℓ, other than B, there is a different Y,B-coordinate system.

   (d) There are as many coordinate systems on a line as there are ordered pairs of distinct points on the line.

   (e) There are exactly two coordinate systems whose base points are found in the set {A,B}, if A $\neq$ B.

(f) There are exactly three coordinate systems on line ℓ whose base points are found in the set $\{A,B,C\}$.

(g) There is exactly one point on line ℓ whose A,B-coordinate is 2562.8.

(h) There is no point on line ℓ whose A,B-coordinate is the same as its B,A-coordinate.

5. We defined the A,B-distance between points P and Q with A,B-coordinates p and q to be $|p - q|$.

   (a) Prove Theorem 1.

   (b) Find possible coordinates of S on $\overleftrightarrow{AB}$ if the A,B-distance from S to B is twice the A,B-distance from S to A.

6.4 Axiom 5. Relating Two Coordinate Systems on a Line

If we brought together an inch-ruler and a foot-ruler, edge to edge, as shown in Figure 6.8, they would suggest two coordinate systems on a line

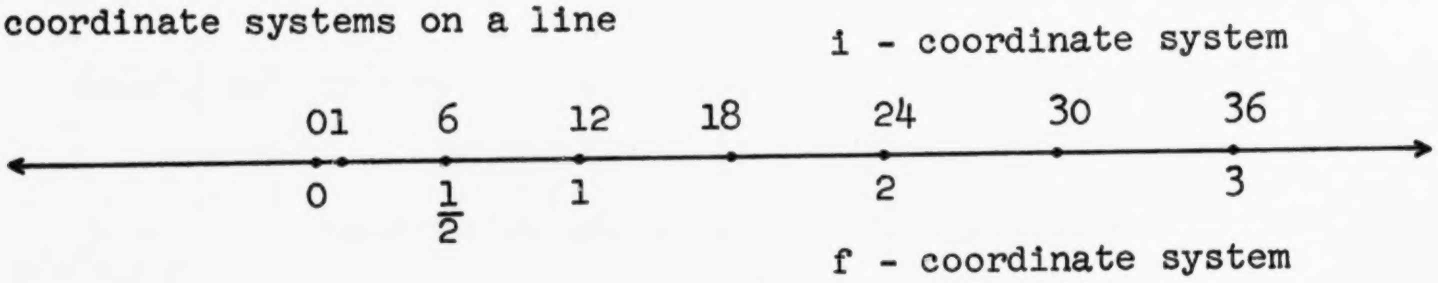


Figure 6.8

Note that they have the same origin, but not the same unit-point. Let us call them the f-coordinate system (foot) and the i-coordinate system (inch). Can we relate the two coordinates of any point? No doubt you see that the i-coordinate of each point is 12 times its f-coordinate. This suggests that the set of f-coordinates can be mapped onto the set of i-coordinates by a dilation given by $i = 12f$. (This applies to all i- and f-coordinates, including negative numbers.)

Let us move the inch-system to the right a distance of 6 inches. Then the two systems appear as in Figure 6.9.

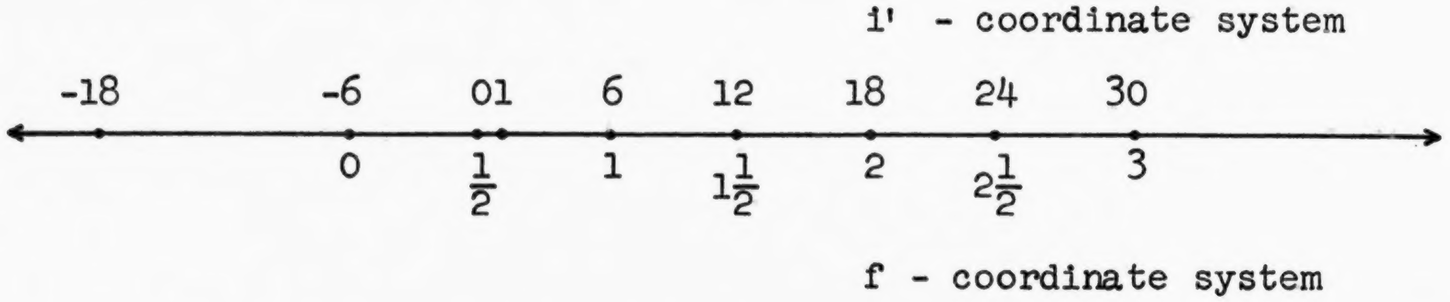


Figure 6.9

To distinguish the two inch-systems, let us call the one shown in Figure 6.9 the i'-coordinate system. If we map f-coordinates by the dilation d used above with rule $f \xrightarrow{d} 12f$, then we note the following:

$$-1 \xrightarrow{d} -12, \quad 0 \xrightarrow{d} 0, \quad 1 \xrightarrow{d} 12, \quad 1\tfrac{1}{2} \xrightarrow{d} 18, \quad 2 \xrightarrow{d} 24.$$

Do you notice that each image has overshot the i'-coordinate in Figure 6.9 by 6? This can be corrected by a translation, call it t, having the rule $x \xrightarrow{t} x - 6$.

The composition of the dilation d followed by the translation t maps f-coordinates onto i'-coordinates. For each value of f the succession of images can be written

$$f \xrightarrow{d} 12f \xrightarrow{t} 12f - 6.$$

Therefore

$$f \xrightarrow{t \circ d} 12f - 6.$$

The rule for converting f values in Figure 6.9 to i' values is therefore

$$i' = 12f - 6.$$

Check this result with f = 2, with $f = 1\frac{1}{2}$.

Recall that i' represents coordinates in an inch-coordinate system and f represents coordinates in a foot-coordinate system. If we generalize what we found for these two coordinate systems to any pair of coordinate systems on a line we have Axiom 5. But we must know how to generalize the formula $i' = 12f - 6$ correctly. To do this we consider any dilation followed by any translation, both on the same line. Any dilation has a rule of the form $x \longrightarrow ax$, where a is any nonzero real number; and any translation has a rule of the form $x \longrightarrow x + b$, where b is any real number. The composition of both mappings then has a rule of the form

$$x \longrightarrow ax + b.$$

Letting x represent the coordinate of any point on the line in one system, and x' its coordinate in the other system, we can write

$$x' = ax + b.$$

We now state Axiom 5 precisely.

Axiom 5. If (A,B) and (A',B') are bases for coordinate systems on a line, then there is a relation $x' = ax + b$ with $a \neq 0$ which, for each point X of the line, relates its A,B-coordinate x to its A',B'-coordinate x'.

The composition of a dilation and a translation on a line is known as an affine mapping or affine transformation on a line. Axiom 5 therefore says that the coordinates of a line coordinate system can be mapped onto the corresponding coordinates of any coordinate system on that line by an affine transformation.

Knowing that there is such a transformation is not the same as knowing what it is. But it helps as we show with an example. Suppose we are given two coordinate systems, as shown in Figure 6.10, and we call the coordinates

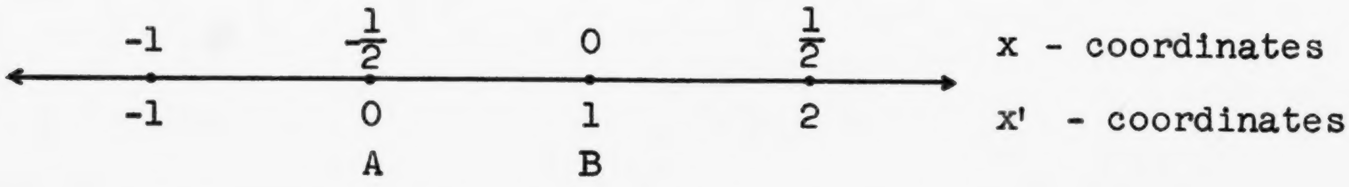


Figure 6.10

shown above the line the x-coordinates, and those below the x'-coordinates. We seek a value of a and a value of b such that for the coordinates x and x of each point, $x' = ax + b$. Axiom 5 tells us there are such values, so we start with $x' = ax + b$. Choosing a point on the line, say A, we replace x and x' by the two coordinates of A. This gives us equation (1). A second point, say B, yields equation (2). As you will see, these two equations are sufficient to lead us to determining the values of a and b. Look at equation (3) and tell how it was obtained from equation (1). How is equation (4) obtained from (2)? Equation (4) tells us that b is 1. Using this information show how equation (5) follows from (3). Finally (6) tells us that a is 2. The formula that should relate the x-coordinates to x'-coordinates is

$x' = ax + b$
(1) $0 = a(-\frac{1}{2}) + b$
(2) $1 = a(0) + b$
(3) $\frac{1}{2}a = b$
(4) $1 = b$
(5) $\frac{1}{2}a = 1$
(6) $a = 2$

$$x' = 2x + 1.$$

Check it with $x = -1$, with $x = \frac{1}{2}$. If you wish to interpret the affine transformation that maps x-coordinates onto x'-coordinates, you can see from the formula that it is the composition of the dilation with rule $x \longrightarrow 2x$, followed by the translation with rule $x \longrightarrow x + 1$. Try to explain how this was determined from the formula $x' = 2x + 1$.

Let us look at another similar problem. The data for this problem are given in Figure 6.11.

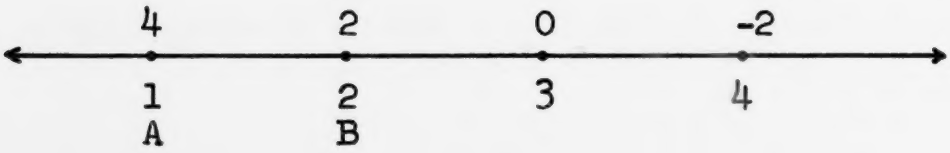


Figure 6.11

We start with $x' = ax + b$. The coordinates of A lead to equation (1). The coordinates of B lead to equation (2). Equation (5) says that $1 - 4a$ and $2 - 2a$ are equal, the reason being that each is the same as b. Study the rest of the solution. Finally we see

$$x' = -\frac{1}{2}x + 3.$$

(1) $1 = a(4) + b$
(2) $2 = a(2) + b$
(3) $1 - 4a = b$
(4) $2 - 2a = b$
(5) $1 - 4a = 2 - 2a$
(6) $-1 = 2a$
(7) $a = -\frac{1}{2}$
(8) $b = 1 - 4(-\frac{1}{2})$ or 3

Check with $x = 0$, with $x = -2$. Describe the affine transformation in terms of a dilation followed by a translation that maps x-coordinates onto corresponding x'-coordinates.

6.5 Exercises

1. The relation between x-coordinates and x'-coordinates in two

systems on a line is $x' = 3x - 1$.

(a) The x-coordinate of point A is 2. What is its x'-coordinate?

(b) The x-coordinate of B is 4. What is its x'-coordinate?

(c) The x'-coordinate of C is 8. What is its x-coordinate?

(d) The x'-coordinate of D is -22. What is its x-coordinate?

(e) Find the x'-coordinate of the point whose x-coordinate is 3000.

(f) Find the x-coordinate of the point whose x'-coordinate is 3000.

(g) Find the x'-coordinate of the point whose x-coordinate is $\sqrt{10}$.

(h) Find the x-coordinate of the point whose x'-coordinate is $\sqrt{11}$.

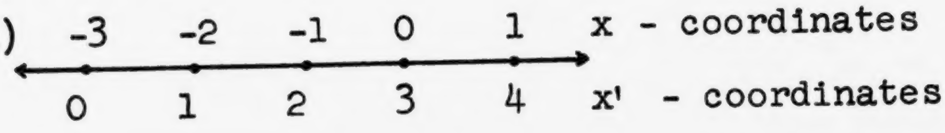
(i) Find the x-coordinate of a point whose x- and x'-coordinates are equal. (Hint: let $x' = x$.)

(j) Find the x-coordinate of a point whose x'-coordinate is twice its x-coordinate.

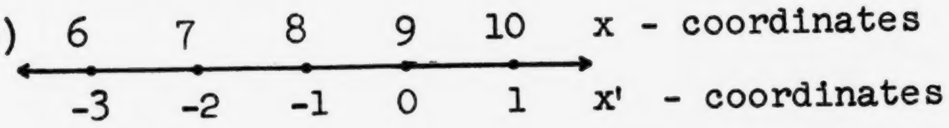
2. Do Exercise 1 for the two coordinate systems on a line with x- and x'-coordinates, if $x' = \frac{1}{2}x + 3$ relates the x-coordinate of any point on the line with the x'-coordinate of that point.

3. For each pair of coordinate systems on a line indicated below, find the formula that converts the x-coordinate of each point to its x'-coordinate. Check each formula with data not used in deriving the formula.

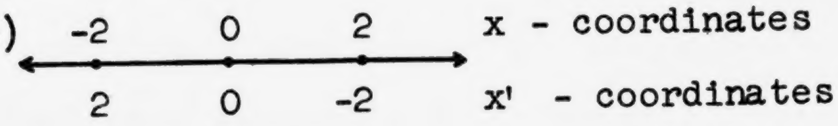
(a)


-3
-2
-1
0
1
x - coordinates
0
1
2
3
4
x' - coordinates

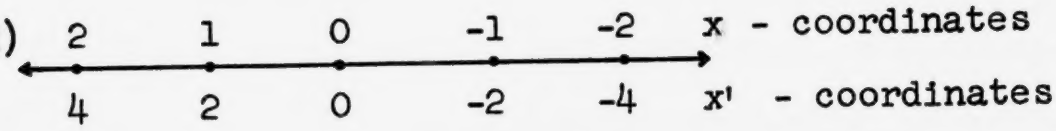
(b)


6
7
8
9
10
x - coordinates
-3
-2
-1
0
1
x' - coordinates

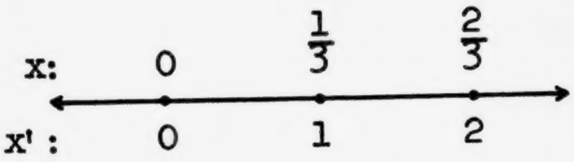
(c)


-2
0
2
x - coordinates
2
0
-2
x' - coordinates

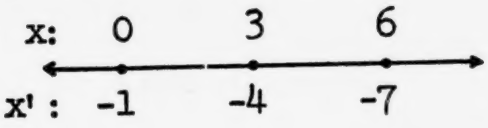
(d)


2
1
0
-1
-2
x - coordinates
4
2
0
-2
-4
x' - coordinates

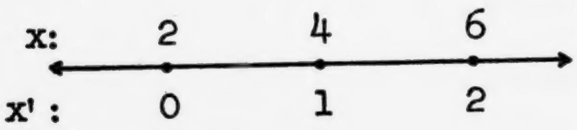
(e)


x:
0
1/3
2/3
x':
0
1
2

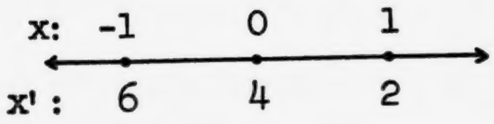
(f)



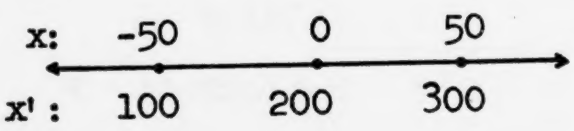
(g)



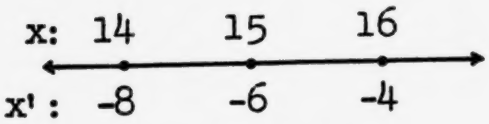
(h)



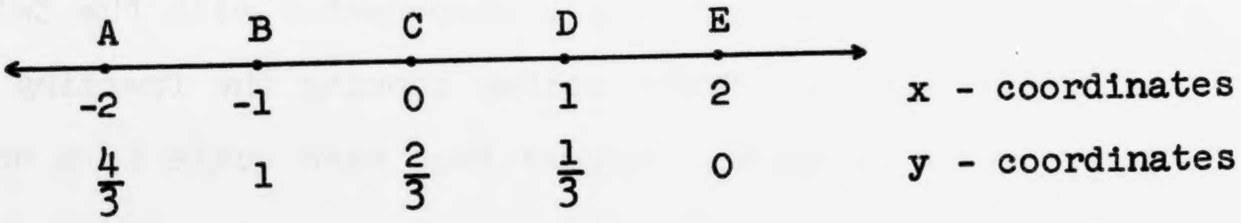
(i)


x:
-50
0
50
x':
100
200
300

(j)


x:
14
15
16
x':
-8
-6
-4

4.

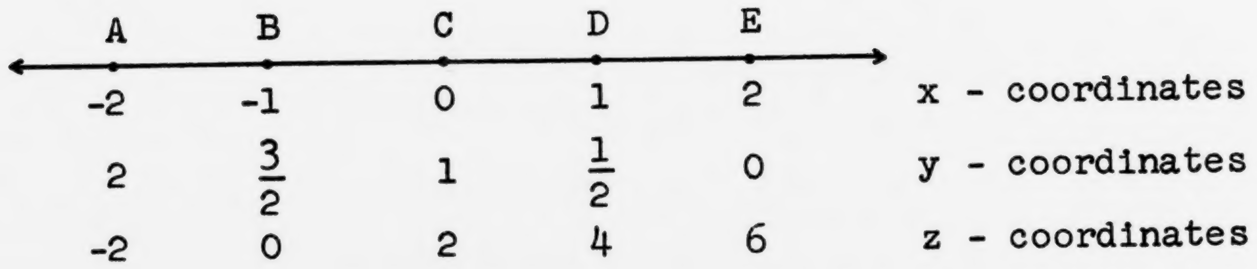

A
B
C
D
E
-2
-1
0
1
2
x - coordinates
4/3
1
2/3
1/3
0
y - coordinates

The diagram above indicates two coordinate systems on a line. Let x be the C,D-coordinate of a point and y the E,B-coordinate of the point.

(a) Find a formula that converts x-coordinates to y-coordinates.

(b) Find a formula that converts y-coordinates to x-coordinates.

5.



A	B	C	D	E	
-2	-1	0	1	2	x - coordinates
2	$\frac{3}{2}$	1	$\frac{1}{2}$	0	y - coordinates
-2	0	2	4	6	z - coordinates

The diagram above indicates three coordinate systems on one line. Using the data shown find a formula that converts

(a) y-coordinates to x-coordinates.

(b) z-coordinates to x-coordinates.

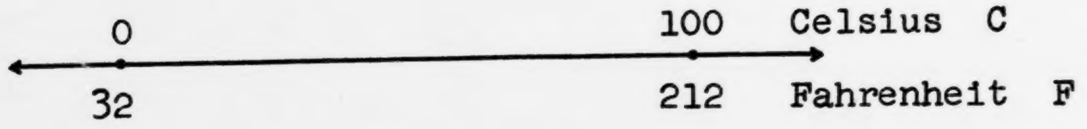
(c) z-coordinates to y-coordinates.

(d) x-coordinates to z-coordinates.

(e) x-coordinates to y-coordinates.

(f) y-coordinates to z-coordinates.

6.



Let the diagram indicate a thermometer with the Celsius (Centigrade) and Fahrenheit scales showing the freezing and boiling points of water. Assume that each scale is a model of a line coordinate system.

(a) Find a formula that converts C-coordinates (Celsius readings) to F-coordinates (Fahrenheit readings).

(b) Find a formula that converts F-coordinates to C-coordinates.

Using the formulas found in a or b, find

(c) the Fahrenheit reading that corresponds to the Celsius reading of 50, -20, 1000.

(d) the Celsius reading that corresponds to the Fahrenheit reading of 50, -14, 2000.

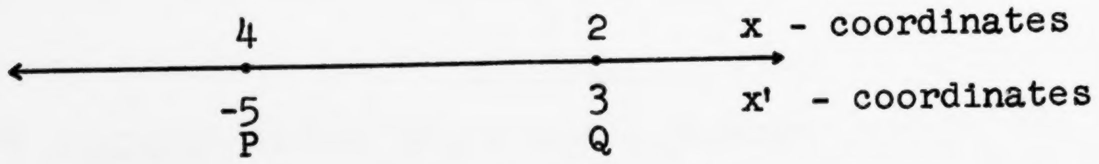
(e) Find the reading for which the F- and the corresponding C-coordinates are the same.

(f) What is the F-coordinate which is 20 more than its corresponding C-coordinate?

(g) What is the name that describes the kind of mapping that relates Fahrenheit and Celsius readings?

7. Given two points A,B. Find the formula that converts A,B-coordinates to B,A-coordinates and find the point whose A,B-coordinate is the same as its B,A-coordinate.

8.



Using the data indicated in the above figure, find the x'-distance between P and Q and the x-distance between P and Q. What is the ratio of these distances? Find the formula $x' = ax + b$ that converts x-coordinates to x'-coordinates and show that the distance ratio is equal to $|a|$.

9. Let points P and Q have coordinates p and q in some coordinate system on $\overleftrightarrow{PQ}$, with base (A,B). Let P and Q have coordinates p' and q' in another coordinate system with base (A',B'), and let $x' = ax + b$ convert A,B-coordinates to A',B'-coordinates. Prove that the A',B'-distance between P and Q is $|a|$ times the A,B-distance between P and Q.

6.6 Segments, Rays, Midpoints

We usually think of segment $\overline{AB}$ (where $A \neq B$) as the set consisting of A, B and the points of $\overleftrightarrow{AB}$ between A and B. Up to now the word "between" has not been defined mathematically; rather we have thought of betweeness of points intuitively, in terms of physical models of points and lines. In this chapter we can define the betweeness relation for points in a line formally, without relying on properties of physical models.

Definition. Point P is between two points A and B, if the A,B-coordinate of P is between 0 and 1.

Definition. If $P \neq Q$, then segment $\overline{PQ}$ is the set of points consisting of P, Q and all points of $\overleftrightarrow{PQ}$ that are between P and Q. P and Q are called endpoints of the segment; the points between P and Q are called interior points of the segment.

We can think of $\overline{AB}$ as the set of points whose coordinates x satisfy $0 \leq x \leq 1$ in the A,B-coordinate system.

Note that we use Axiom 4 to introduce the coordinate system in which A and B have coordinates 0 and 1 respectively, and then we rely on our knowledge of the betweeness relation for numbers, in terms of inequalities.

Thus, if p is the coordinate of P in the A,B-coordinate system, then P is between A and B if and only if $0 < p < 1$. But you probably ask, suppose we look at A, B, and P from the point of view of another coordinate system in which the coordinate of P is between the coordinates of A and B in the second system, will P be between A and B? Axiom 5 helps to answer this question.

We show how with a particular example. Suppose A and B have coordinates 7 and -3 as shown in Figure 6.12, and P has a coordinate x between 7 and -3.

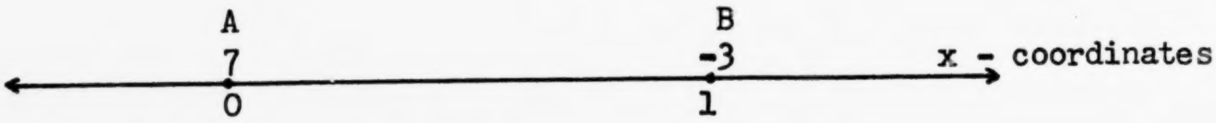


Figure 6.12

Will P be between A and B, as defined above? To answer we should find the A,B-coordinate of P. To do this we first find the formula $x' = ax + b$ that converts the x-coordinate of A to 0 and the x-coordinate of B to 1. This means finding an a and a b such that $0 = a\cdot 7 + b$ and $1 = a(-3) + b$. Solving, as we did in Section 6.4, we get $a = -\frac{1}{10}$ and $b = \frac{7}{10}$. The coordinate of P, x, satisfies condition (1) at the right. Now we convert x-coordinates to A,B-coordinates by the formula: A,B-coordinate $= -\frac{1}{10}x + \frac{7}{10}$. The first step is to multiply by $-\frac{1}{10}$. This produces (2). Why is the order reversed? Then adding $\frac{7}{10}$, we get (3), which shows that the A,B-coordinate of P is between 0 and 1. We conclude that P is between A and B, in accordance with our definition.

(1) $-3 < x < 7$

(2) $-\frac{7}{10} < -\frac{1}{10}x < \frac{3}{10}$

(3) $0 < -\frac{1}{10}x + \frac{7}{10} < 1$

The definition we gave for a line segment is now on sound mathematical ground. Moreover, we can use any coordinate system to define a segment. For instance, using x-coordinates in Figure 6.12 we can say:

$\overline{AB}$ is the set of points whose x-coordinates satisfy the condition $-3 \leq x \leq 7$.

Or we can say

$\overline{AB}$ is the set of points whose A,B-coordinates x' satisfy the condition $0 \leq x' \leq 1$.

We can also use Axioms 4 and 5 to give a precise definition for ray.

Definition. If P and Q are distinct points of a line ℓ, then the subset of ℓ whose P,Q-coordinates x satisfy the condition $x \geq 0$ is called a ray, designated $\overrightarrow{PQ}$. The point P is the endpoint of the ray, and all of its remaining points are called interior points of the ray.

If we convert these x-coordinates by the dilation with formula $x' = -x$, we are led to another coordinate system with the same origin as the x-coordinate system. Applying our definition of a ray to the x'-coordinate system we see that the set of points with x'-coordinates satisfying $x' \geq 0$ is also a ray. Thus the point P serves as a common endpoint of two rays whose interiors have no points in common. Naturally, we call them opposite rays.

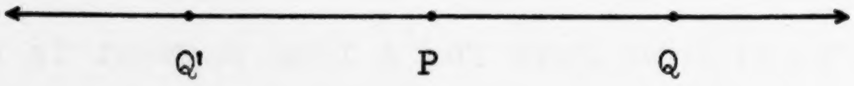


Figure 6.13

$\overrightarrow{PQ}$ and $\overrightarrow{PQ'}$ are opposite rays

We know now that the coordinates x of the points of $\overrightarrow{PQ}$ satisfy the condition $x \geq 0$ in the P,Q-coordinate system on $\overleftrightarrow{PQ}$. You might reasonably ask what condition these coordinates would satisfy in other coordinate systems on $\overleftrightarrow{PQ}$. By Axiom 5, the coordinate x' of a point in another coordinate system is related to the coordinate x of the same point in the P,Q-coordinate system by an affine transformation $x' = ax + b$, with $a \neq 0$. Thus $a < 0$ or $a > 0$. In either case $x \geq 0$. Computing:

$$\begin{array}{rcr} x \geq 0 & \qquad & x \geq 0 \\ a > 0 & & a < 0 \\ ax \geq 0 & & ax \leq 0 \\ ax + b \geq b & & ax + b \leq b \end{array}$$

(Do you see why $x \geq 0$ and $a < 0$ implies $ax \leq 0$?) We conclude that in any coordinate system, the points of $\overrightarrow{PQ}$ satisfy a condition $x \geq b$ or $x \leq b$ (but not both).

If you look back at Course 1, Chapter 10, Section 10.2, you will find that we first introduced rays there, and then defined $\overline{AB}$ as $\overrightarrow{AB} \cap \overrightarrow{BA}$. In this chapter $\overrightarrow{AB}$ and $\overrightarrow{BA}$ are the sets of points whose A,B-coordinates satisfy $x \geq 0$ and $x \leq 1$, respectively. (Verify this.) Thus in this chapter, $\overrightarrow{AB} \cap \overrightarrow{BA}$ is the set of points whose A,B-coordinates x satisfy $0 \leq x \leq 1$, which is of course $\overline{AB}$.

Theorem 2. If C is between P and Q, then the A,B-distance between P and C, plus the A,B-distance between C and Q, is equal to the A,B-distance between P and Q.

The "then" part of this theorem can be written $PC + CQ = PQ$.

Proof. Exercise

You have probably anticipated the definition of a midpoint of a segment.

Definition. The midpoint of $\overline{AB}$ is the point whose A,B-coordinate is $\frac{1}{2}$.

But you will probably ask, what will its coordinate be in any other coordinate system? Let us see. Suppose in the x'-coordinate system the x'-coordinates of A and B are respectively a and b. (See Figure 6.14)

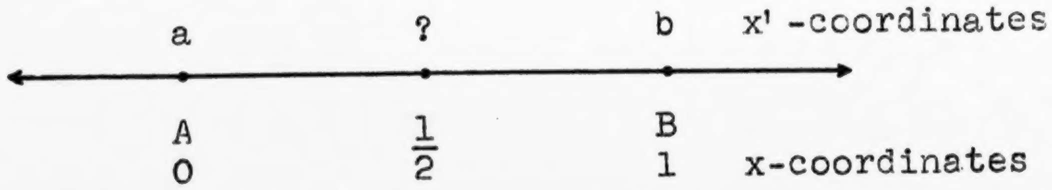


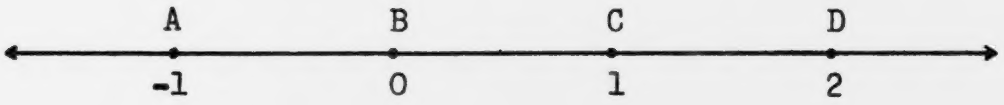
Figure 6.14

You can check that $x' = (b - a)x + a$ converts x-coordinates to x'-coordinates. What is x' when $x = 0$? when $x = 1$? Thus the x'-coordinate of the mid-point of $\overline{AB}$ is found by replacing x by $\frac{1}{2}$. Show that the result is $x' = \frac{a + b}{2}$. This proves a theorem we shall find useful.

Theorem 3. (Midpoint) If the coordinates of A and B are a and b respectively in some line coordinate system, then the coordinate of the midpoint of $\overline{AB}$, in that system, is $\frac{a + b}{2}$.

You can recall this formula easily if you think of $\frac{a + b}{2}$ as the mean or average of a and b.

6.7 Exercises



1. Using the data indicated in the above diagram for a line coordinate system, and letting x represent coordinates in that system, write the inequality or equality that is satisfied by the coordinate(s) of the points in each of the following:

   (a) $\overline{AC}$ (b) $\overline{AD}$ (c) $\overline{DC}$ (d) $\overrightarrow{AD}$

   (e) $\overrightarrow{CA}$ (f) $\overrightarrow{CB}$ (g) the midpoint of $\overline{AC}$

   (h) the midpoint of $\overline{AD}$ (i) $\overline{AC} \cap \overline{BD}$ (j) $\overline{AC} \cup \overline{CD}$

2. Find the x-coordinate of the midpoint of $\overline{AB}$ if the x-coordinates of A and B are the following pairs of numbers:

   (a) 3 and 8 (b) -3 and 8 (c) -3 and -8

   (d) 3 and -8 (e) 152 and -152 (f) $\frac{1}{2}$ and $\frac{1}{3}$

   (g) $-2\frac{1}{2}$ and $3\frac{1}{5}$ (h) 8.2 and -3.6 (i) $\sqrt{2}$ and $\sqrt{3}$

3. In a certain coordinate system the coordinate of A is 3. Find the coordinate of B if the midpoint of $\overline{AB}$ has coordinate:

   (a) 8 (b) -8 (c) 0 (d) $\sqrt{2}$

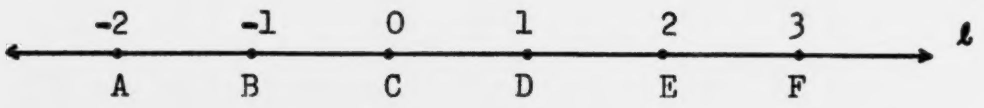
4. Below are sets of three points on a line. Each is accompanied by its coordinate in a certain coordinate system on the line. For each set tell which point is between the other two.

   (a) A -12, B -4, C 1. (b) P $\sqrt{2}$, Q $\sqrt{3}$, R 1.5.

(c) L $-3\frac{1}{2}$, M -3.5, N -3.4. (d) D $\sqrt{2} - \sqrt{2}$, E 0,
F $\sqrt{3} - \sqrt{2}$.

5. Consider three coordinate systems on a line, the first having x-coordinates, the second y-coordinates, and the third z-coordinates. If the formula $y = 3x - 2$ converts x- to y-coordinates and the formula $z = \frac{1}{2}y + 1$ converts y- to z-coordinates, find the formula that converts x-coordinates to z-coordinates.

6.



Let $\underline{x}$ represent the C,D-coordinates of a point X on line ℓ. Using names of points of ℓ, designate the subsets of ℓ listed below. The first of these is read: the set of points X such that their x-coordinates satisfy the condition $x \geq -1$.

(a) $\{X: \ x \geq -1\}$ (b) $\{X: \ x \leq 3\}$ (c) $\{X: \ x = 3\}$
(d) $\{X: \ 0 \leq x \leq 2\}$ (e) $\{X: \ -2 \leq x \leq x\}$
(f) $\{X: \ x > 1\}$ (g) $\{X: \ 0 < x \leq 2\}$ (h) $\{X: \ -2 < x < -1\}$

7. Using coordinates prove that if point X is in $\overline{AB}$, then X is in $\overrightarrow{AB}$.

8. Using coordinates prove that if distinct points X and Y are interior points of $\overline{AB}$, then every point of $\overline{XY}$ is an interior point of $\overline{AB}$.

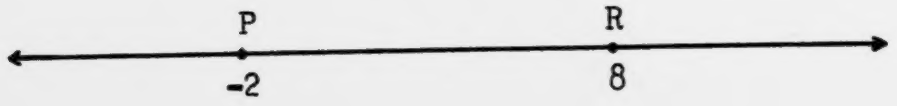
9. Prove Theorem 2.

*10. Let P, Q, R be points of a line with P distinct from R, having respective coordinates $\underline{p}$, $\underline{q}$, $\underline{r}$, in some coordinate system. We call the ratio $\frac{q - p}{r - p}$ the *ratio in which* Q *divides* $\overline{PR}$ *from* P *to* R.

(a) What is the special name given to Q if $\frac{q - p}{r - p} = \frac{1}{2}$? If you have difficulty answering, solve for q in terms of p and q.

(b) Find an interpretation for Q if $\frac{q - p}{r - p} = \frac{1}{3}, \frac{2}{3}$.

(c) Point Q is an interior point of $\overline{PR}$ if $m < \frac{q - p}{r - p} < n$. What are the values of m and n?



Check your answer with $p = -2$ and $r = 8$ as shown above. When Q is between P and R we say that Q divides $\overline{PR}$ *internally*.

(d) Using the data in (c) and a coordinate of Q for which P is between Q and R, find $\frac{q - p}{r - p}$. Is the value negative? Show that P is between Q and R if $\frac{q - p}{r - p} < 0$.

(e) Show that R is between P and Q if $\frac{q - p}{r - p} > 1$.
When Q is not between P and R, then we say that Q divides $\overline{PR}$ *externally*.

(f) Show that $\frac{q - p}{r - p}$ does not change when p, q, and r are replaced by their images under an affine transformation. (Hint: Use the rule $x' = ax + b$. Then q is replaced by $aq + b$, etc.)

(g) Prove: $\frac{q - p}{r - p}$ is the P,R-coordinate of Q.

(h) Prove that $\frac{q - p}{r - p} = 0$ if and only if $Q = P$, and that $\frac{q - p}{r - p} = 1$ if and only if $Q = R$.

6.8 Axiom 6. Parallel Projections and Line Projections

We need only one more axiom to complete the set of axioms.

Let ℓ and ℓ' be any two lines in a plane, and take (A,B) as base of a coordinate system on ℓ. (See Figure 6.15.)

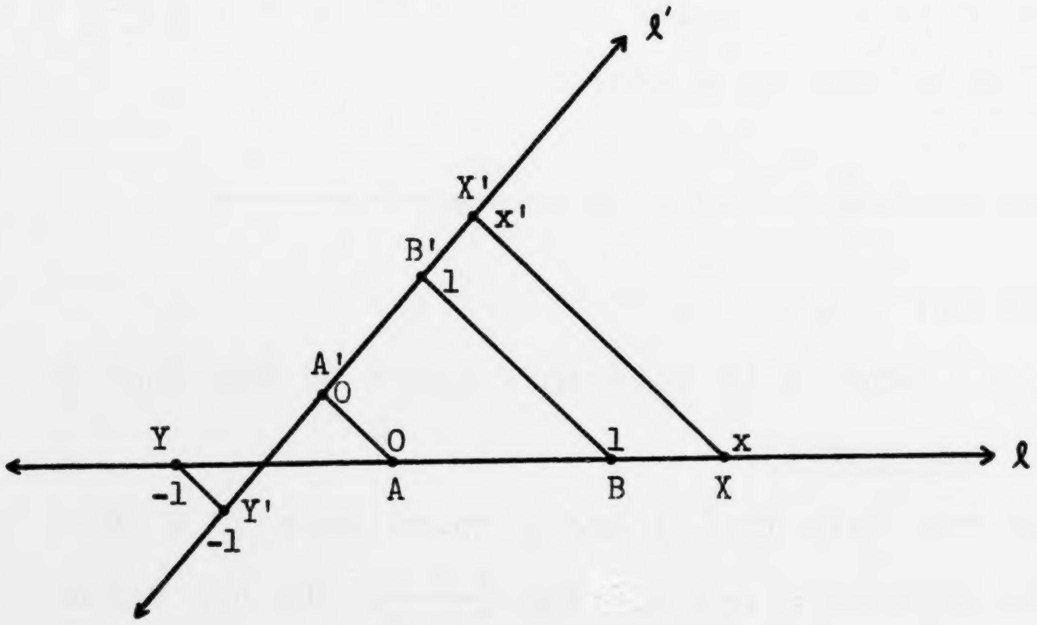


Figure 6.15

Consider a parallel projection from ℓ to ℓ'; call it f. (See Chapter 3, Section 3.12) Then $A \xrightarrow{f} A'$, $B \xrightarrow{f} B'$. Let (A', B') be the base of a coordinate system of ℓ'. If X has A,B-coordinate $1\frac{1}{2}$ and $X \xrightarrow{f} X'$, it seems reasonable that the A', B'-coordinate of X' is also $1\frac{1}{2}$. If Y has A,B-coordinate -1, and $Y \xrightarrow{f} Y'$, it seems likely that the A',B'-coordinate of Y' is also -1, and so on for all points of ℓ and their images in ℓ' under f.

We can describe this state of affairs by saying that parallel projections preserve relative positions of points and ratios of distances. To put it briefly, parallel projections preserve coordinate systems. This is the content of Axiom 6, which we now state precisely.

Axiom 6. Let f be a parallel projection from line ℓ to line ℓ'. Let A,B be distinct points of ℓ and let A',B' be their images under f. Then for every point X of ℓ, the A', B'-coordinate of its image, X', is the same as the A,B-coordinate of X.

An immediate consequence of this axiom is the following theorem.

Theorem 4. Under a parallel projection from line ℓ to line ℓ',

(a) the set of images of the points of a segment on ℓ is a segment.

(b) the image of the midpoint of a segment is the midpoint of the image segment.

(c) the set of images of the points in a ray is a ray.

Proof. Exercise.

For convenient reference in working the exercises, we restate the six axioms.

Axiom 1. (a) Plane π is a set of points, and it contains at least two lines.

(b) Each line in plane π is a set of points, containing at least two points.

Axiom 2. For every two points in plane π there is one and only one line in π containing them.

Axiom 3. For every line m and point E in the plane π, there is one and only one line in π containing E and parallel to m.

Axiom 4. For each pair of distinct points A and B of a line there is exactly one coordinate system on that line in which A corresponds to 0 and B corresponds to 1.

Axiom 5. If (A,B) and (A',B') are bases for coordinate systems on a line, then there is a relation $x' = ax + b$ with $a \neq 0$ which, for each point X of the line, relates its A,B-coordinate x to its A',B'-coordinate x'.

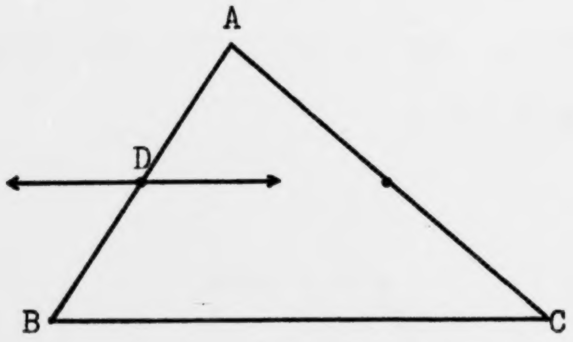
Axiom 6. Let f be a parallel projection from line ℓ to to line ℓ'. Let A,B be distinct points of ℓ and let A',B' be their images under f. Then for every point X of ℓ, the A',B'-coordinate of its image, X', is the same as the A,B-coordinate of X.

6.9 Exercises

In Exercises 1 - 5 assume that f is a parallel projection from line ℓ to line ℓ'; that A, B, C are points of ℓ; that their respective images under f are A', B', C'; and that A and C are distinct points.

1. Prove that B' is between A' and C' if B is between A and C.
2. Prove: If B is the midpoint of $\overline{AC}$, then B' is the midpoint of $\overline{A'C'}$.

3. Prove: The image of $\overrightarrow{AC}$ is a ray.
4. Let B divide $\overline{AC}$, from A to C, in the ratio r. Prove that B' divides $\overline{A'C'}$, from A' to C', in the ratio r.
5. Prove: the ratio of the A,B-distance from A to C to the A,B-distance from C to B is equal to the ratio of the A',B'-distance from A' to C' to the A',B'-distance from C' to B'. This theorem is sometimes known as Thales' theorem, after the Greek mathematician Thales (c. 624 - 548 B.C.) who is called the father of geometry.
6. A, B, C are three non collinear points with D the midpoint of $\overline{AB}$, as shown below. Prove that the line containing D and parallel to $\overleftrightarrow{BC}$ passes through the midpoint of $\overline{AC}$.



7. Modify the data in Exercise 6 to the effect that D is the trisection point nearer A, and prove the appropriately modified conclusion.

6.10 Plane Coordinate Systems

You saw how line coordinate systems enable us to prove theorems about sets of points on a line. In this section we construct another kind of coordinate system, this time for a plane, and you may expect that it will enable us to prove theorems about point sets in a plane. As we construct a plane coordinate system, it will be instructive to note analogies between line coordinate systems and plane coordinate systems. We urge you to look for them.

We start by choosing any ordered triple of three non collinear points in a plane. Let us name it (O,I,J) and call the ordered triple the base of the system. We call $\overleftrightarrow{OI}$ the x-axis, and $\overleftrightarrow{OJ}$ the y-axis. On the x-axis, base (O,I) determines a line coordinate system. On the y-axis, base (O,J) determines a line coordinate system. It may surprise you that this is all the equipment we need to assign to every point in the plane an ordered pair of numbers. We illustrate how this is done for point P. (See Figure 6.16.)

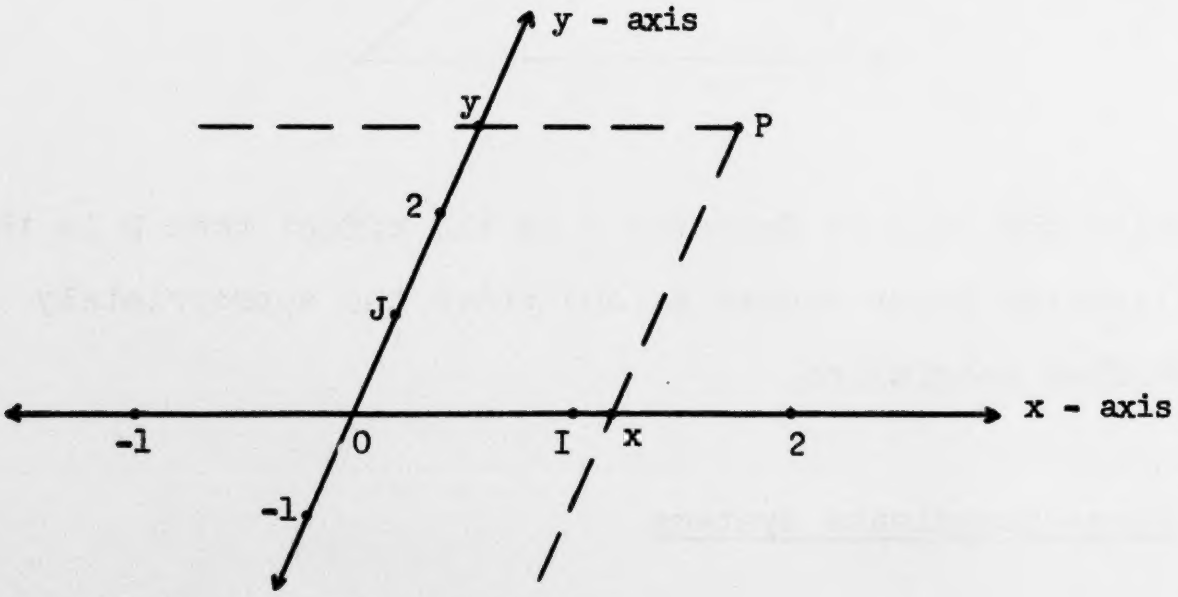


Figure 6.16

Consider the line through P parallel to $\overleftrightarrow{OJ}$. Is there one? More than one? Why? This line intersects $\overleftrightarrow{OI}$ in exactly one point. See Chapter 3, Section 3.5, Theorem 10, for the justification of this assertion. Let this point have O,I-coordinate x. x is assigned to P. In the same manner, by considering the line through P parallel to $\overleftrightarrow{OI}$ and noting its intersection with $\overleftrightarrow{OJ}$ we assign the O,J-coordinate y of this point to P also. The pair of coordinates, in the order mentioned, (x,y), is called the O,I,J-coordinates of P. The first of these, x, is called the x-coordinate of P; the second, y, is called the y-coordinate of P. It is clear from this description that to each point of the plane there corresponds exactly one such ordered pair of numbers.

Let us reverse the procedure. Given an ordered pair of real numbers, (a,b), is there exactly one point that has O,I,J-coordinates (a,b)? The answer is "yes" and we leave the proof of this assertion as an exercise.

The net result of this discussion is this: For every choice of base (O,I,J) in a plane the method by which we assign an ordered pair of real numbers to a point of the plane produces a one-to-one correspondence between the set of points in the plane and the set of ordered pairs of real numbers. The significance of this close kinship between points of a plane and ordered pairs of numbers lies in this fact: Once we have chosen a base for a plane coordinate system, we can identify precisely and clearly any point or any set of points of the plane. For this reason we can study points by studying their plane coordinates. In fact, we name a point such as P, along with its coordinates, say (2,-3), and write them together in the symbol "P(2,-3)." It is read: the point P with coordinates (2,-3). Also we can designate a set of points such as $\{P(x,y): x > 0 \text{ and } y > 0\}$; and this is read: the set of points P with coordinates (x,y) such that x is greater than zero and y is greater than zero. You have probably noted that these points are the interior points of $\angle IOJ$. This set is called the first quadrant of the O,I,J-coordinate system. Let us look at some other examples of point sets.

Example 1. Each point in the x-axis has 0 as its y-coordinate, and its x-coordinate can be any number. Therefore x-axis = $\{P(x,y): y = 0, x \text{ is any real number}\}$.

Example 2. By the positive x-axis we mean $\overrightarrow{OJ}$ without point O. Using coordinates we can describe it as $\{P(x,y): x > 0, y = 0\}$.

Example 3. Consider the segment whose end points are A(-2,2) and B(3,2). Since both points have 2 as y-coordinate they must be in the line which is parallel to the x-axis and passes through the point of $\overleftrightarrow{OJ}$ whose O,J-coordinate is 2. (See Figure 6.17.)

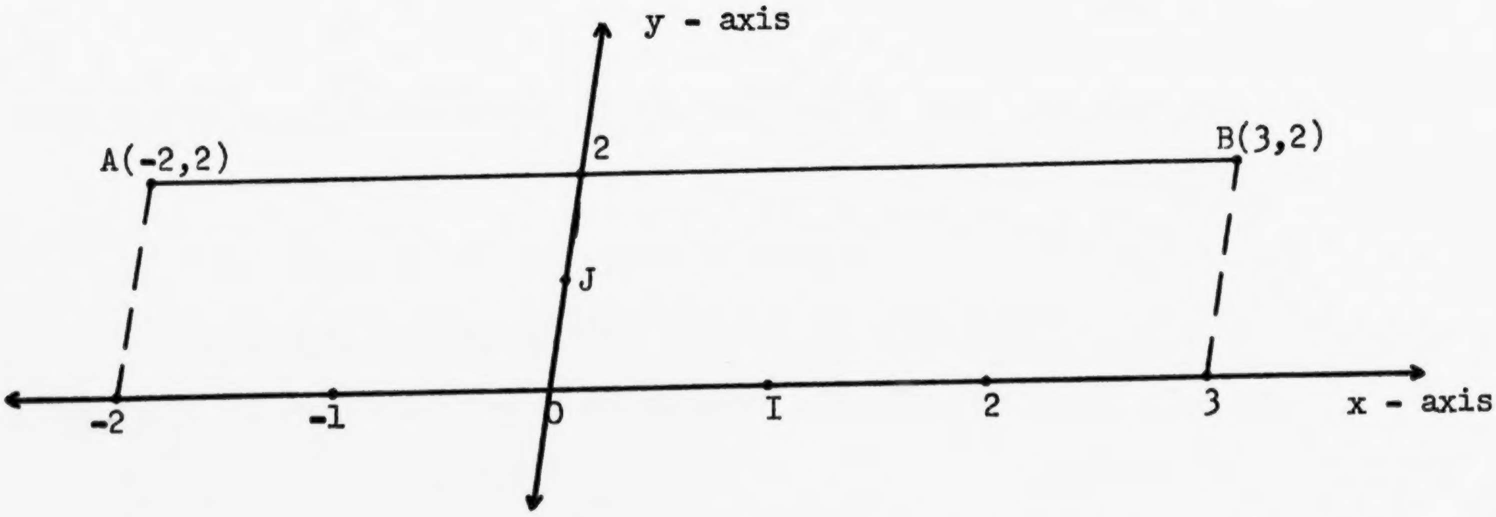

y - axis
A(-2,2)
2
B(3,2)
J
-2
-1
0
I
2
3
x - axis

Figure 6.17

Therefore all points of $\overline{AB}$ have y-coordinate 2. Do you see that all x-coordinates of points in $\overline{AB}$ satisfy the condition $-2 \leq x \leq 3$? Then $\overline{AB} = \{P(x,y): -2 \leq x \leq 3 \text{ and } y = 2\}$.

Example 4. Figure 6.18 is a graph of $\{P(x,y): 0 \leq x \leq 2 \text{ and } -1 \leq y \leq 3\}$. Study it carefully, noting that it is the shaded region. Note carefully how the base (O,I,J) was chosen before studying the graph.

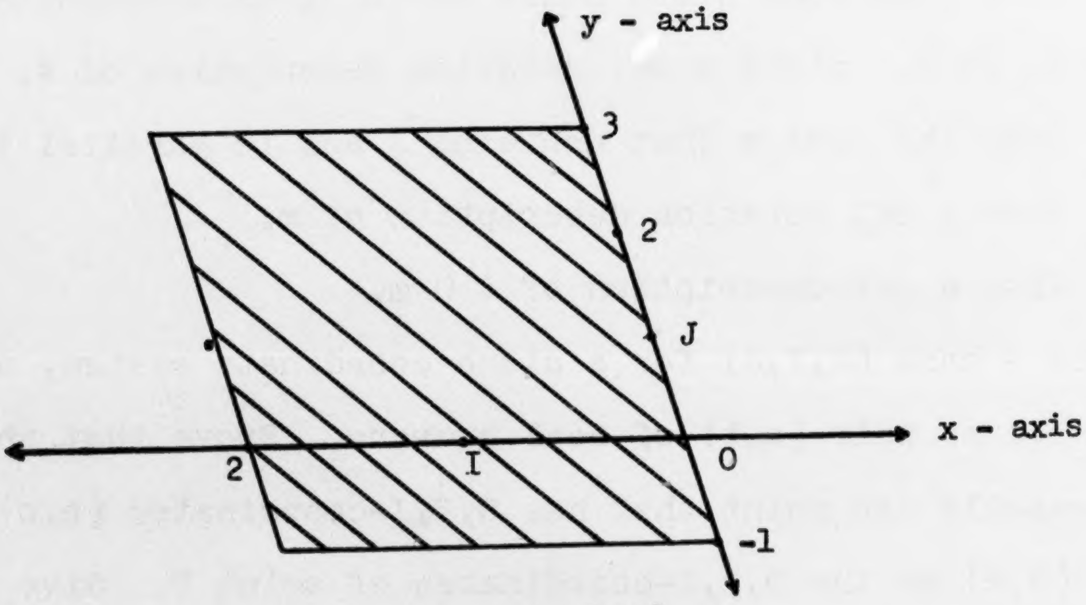

y - axis
3
2
J
x - axis
2
I
0
-1

Figure 6.18

6.11 Exercises

1. Explain why the set of points on the y-axis can be described as $\{P(x,y): x = 0\}$.
2. Where do we find all points belonging to $\{P(x,y): y = 0$ and $x < 0\}$. This set is called the negative x-axis.
3. Using set notation give a reasonable description of each of the following:
   (a) the y-axis.
   (b) the positive y-axis.
   (c) the negative y-axis.
   (d) the second quadrant. (Hint: It contains $P(-2,5)$.)
   (e) the third quadrant. (Hint: It contains $P(-3,-7)$.)
   (f) the fourth quadrant.
4. Choose a base (O,I,J) for a coordinate system on your paper and draw the line that contains I and is parallel to $\overleftrightarrow{OJ}$; call it ℓ.
   (a) Show that every point in ℓ has 1 as x-coordinate. Also show that every point having 1 as x-coordinate is on ℓ. Write a set notation description of ℓ.
   (b) Draw the line m that contains J and is parallel to $\overleftrightarrow{OI}$. Give a set notation description of m.
   (c) Give a set description of $\ell \cap m$.
5. Given a base (O,I,J) for a plane coordinate system, and an ordered pair (a,b) of real numbers. Prove that there is exactly one point that has O,I,J-coordinates (a,b).
6. Let (3,4) be the O,I,J-coordinates of point P. Give

a set notation description of the line that contains P and

(a) is parallel to $\overleftrightarrow{OI}$.

(b) is parallel to $\overleftrightarrow{OJ}$.

(c) Describe, in words, the set $\{Q(x,y)\colon\ y > 4 \text{ and } x > 3\}$.

(d) Describe also $\{R(x,y)\colon\ y \leq 4,\ x > 3\}$.

7. Repeat Exercises 6(a) and 6(b) for the point P whose O,I,J-coordinates are $(-3,2)$.

8. Repeat Exercises 6(a) and 6(b) for the point P whose O,I,J-coordinates are $(-4,-5)$.

9. Make a drawing of each of the following sets using a plane coordinate system of your choice.

   (a) $\{P(x,y)\colon\ x > 0,\ y = 2\}$

   (b) $\{P(x,y)\colon\ x \geq 0,\ y = -4\}$

   (c) $\{P(x,y)\colon\ x = 0,\ y \leq 3\}$

   (d) $\{P(x,y)\colon\ x = 3,\ -1 \leq y \leq 2\}$

   (e) $\{P(x,y)\colon\ y = -2,\ -2 \leq x \leq 2\}$

   (f) $\{P(x,y)\colon\ x < 2,\ y \geq 1\}$

   (g) $\{P(x,y)\colon\ y < 2,\ x \geq 1\}$

   (h) $\{P(x,y)\colon\ -2 \leq x \leq 2,\ -2 \leq y \leq 2\}$

   (i) $\{P(x,y)\colon\ -2 \leq x \leq 2,\ -3 \leq y \leq 3\}$

10. Draw an (O,I,J)-coordinate system and a line ℓ that intersects the y-axis. Consider only the x-coordinates of points on ℓ. Show that the correspondence between the set of these x-coordinates and the set of points on ℓ is a line coordinate system.

6.12 An Equation for a Line

Your work in Section 6.10 and 6.11 no doubt convinced you that some sets of points can be defined precisely in set notation by using equations, inequalities or both. In particular, we used equations to describe sets of points on lines parallel to the x-axis or the y-axis. In this section we look into the question of whether other lines, lines that intersect both axes, can also be described in set notation using equations. Let us try to find the answer for a particular line, and then for any line.

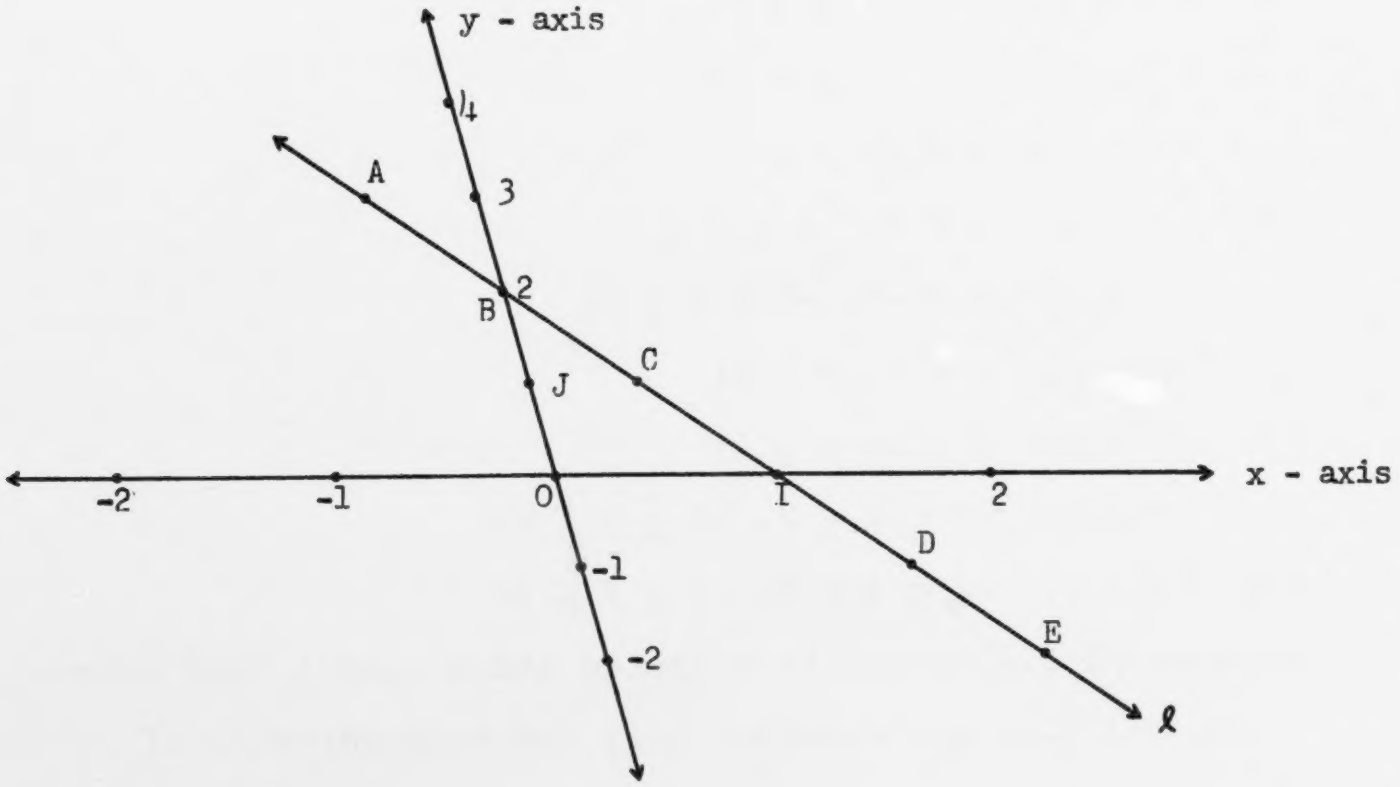


Figure 6.19

In Figure 6.19 line ℓ contains points A,B,C,I,D,E, among others. The coordinates of the named points are recorded in the table below.

	A	B	C	I	D	E
x - coordinate	$-\frac{1}{2}$	0	$\frac{1}{2}$	1	$1\frac{1}{2}$	2
y - coordinate	3	2	1	0	-1	-2

While the table shows x-coordinates of only 6 points, let it suggest the set of x-coordinates of all points of ℓ. By Axiom 6 the correspondence between the set of x-coordinates and points of ℓ is a line coordinate system. (See Exercise 10 of Section 6.11). So too, is the correspondence between the set of y-coordinates and points of ℓ. Hence we have here two coordinate systems on ℓ. By Axiom 5 there is an equation $y = ax + b$ that relates y-coordinates to x-coordinates. It is a simple problem to find a and b. By a method we have already studied, $a = -2$ and $b = 2$. (Check this with the coordinates in the above table.) Thus the coordinates of all points of ℓ satisfy $y = -2x + 2$. But we cannot claim, yet, that $\ell = \{P(x,y): y = -2x + 2\}$, for there may be a point not on ℓ, whose coordinates (x,y) also satisfy $y = -2x + 2$. To show that this cannot be, we argue as follows: For each number p there is a point S on ℓ that has p as x-coordinate. (Why?) There is exactly one number q such that (p,q) satisfies $y = -2x + 2$. (Why?) Therefore S must have q as y-coordinate. We conclude that all points whose coordinates satisfy $y = -2x + 2$ are on ℓ. We are now justified in writing

$$\ell = \{P(x,y): y = -2x + 2\}.$$

The argument we gave for ℓ is the same for any line in the plane that cuts both axes. We call the equation used in set notation to describe ℓ as an equation for ℓ. Note we said an, not the, for there are other equations which can also be used to describe ℓ. For instance, $2x + y = 2$, or $4x + 2y = 4$, or $1000y + 2000x - 2000 = 0$. Do you see that these equations are equivalent to $y = -2x + 2$. Note: $\{(x,y): y = -2x + 2\} = \{(x,y): 4x + 2y = 4\}$.

In Sections 6.10 and 6.11 we saw that we can use an equation of the form $x = r$ to describe lines parallel to the y-axis, and equations of the form $y = s$ to describe lines parallel to the x-axis. We can therefore claim that every line has an equation of the form $ax + by + c = 0$. For lines parallel to the x-axis $a = 0$, and $b \neq 0$. For lines parallel to the y-axis $a \neq 0$, and $b = 0$. For all other lines $a \neq 0$ and $b \neq 0$.

We end this section with three examples in which set notation is used to describe a line, when we know the O,I,J-coordinates of two of its points. Why are only two points needed?

Example 1. Line ℓ contains $A(3,-2)$ and $B(3,7)$.
Since $\overleftrightarrow{AB} \parallel \overleftrightarrow{OJ}$, $\ell = \{P(x,y): x = 3\}$.

Example 2. Line m contains $A(3,-2)$ and $C(8,-2)$.
Since $\overleftrightarrow{AC} \parallel \overleftrightarrow{OI}$, $m = \{P(x,y): y = -2\}$.

Example 3. Line n contains $P(-1,2)$ and $Q(3,1)$.
Assuming both $(-1,2)$ and $(3,1)$ satisfy $y = ax + b$, we get (1) and (2) below. Study the rest of the solution.

(1) $2 = -a + b$

(2) $1 = 3a + b$

(3) $2 + a = b = 1 - 3a$

(4) $4a = -1$

(5) $a = -\frac{1}{4}$

(6) $2 = \frac{1}{4} + b$

(7) $b = \frac{7}{4}$

Therefore $n = \{R(x,y)\colon\ y = -\frac{1}{4}x + \frac{7}{4}\}$.

6.13 Exercises

Assume that all coordinates and equations in these exercises are related to a plane coordinate system with base (O,I,J).

1. A line ℓ has an equation $3x + 2y - 6 = 0$. For each point listed below, determine whether or not it is a point of ℓ.

   (a) $A(0,3)$ (b) $B(2,0)$ (c) $C(2,3)$ (d) $D(-2,6)$

   (e) $E(4,6)$ (f) $F(4,-3)$ (g) $G(1,\frac{3}{2})$ (h) $H(1,-\frac{3}{2})$

   (i) $K(10,12)$ (j) $L(10,-12)$ (k) $M(\frac{1}{2},\frac{9}{4})$ (l) $N(2\sqrt{2}, 3 - 3\sqrt{2})$

2. Which of the following can be an equation for a line?

   (a) $4x - 2y + 5 = 0$ (b) $4x^2 - 2y + 5 = 0$

   (c) $4x - y^2 + 5 = 0$ (d) $x\sqrt{3} = 5$

   (e) $x\sqrt{2} + 5y = 9$ (f) $\pi y = \sqrt{2}$

3. For each equation listed below, write an equivalent equation having the form $y = ax + b$, if possible.

   (a) $3x = 5 - y$ (b) $8 = 3x + y$

   (c) $3x = 8$ (d) $5y = 2$

   (e) $x + \frac{1}{2}y = 4$ (f) $ax + by = c$

4. For each equation of a line listed below, find the coordinates of a point that is on the line, and the coordinates of a point that is not on the line.

   (a) $2x + 3y = 6$ (b) $2x - 3y = 12$

   (c) $x + \frac{1}{2}y = 4$ (d) $3x = 28$

   (e) $\frac{1}{2}x + \frac{1}{3}y = 4$ (f) $5y = \sqrt{3}$

5. Determine whether or not, for each equation listed below, the line for which it is equation contains point $P(2,-3)$.

   (a) $x = 2$ (b) $y = -3$ (c) $x + y = -1$

   (d) $x - y = -1$ (e) $\frac{1}{2}x - \frac{1}{3}y = 0$ (f) $\frac{1}{2}x + \frac{1}{3}y = 0$

   (g) $3x + 2y = 6$ (h) $3x + 2y = 0$ (i) $\frac{4}{2}x + \frac{4}{3}y = 0$

   (j) $2x + y + 1 = 0$ (k) $3x + 2y + 1 = 0$ (l) $\sqrt{2}x - \sqrt{3}y = 2$

6. Which of the following lines pass through O, which pass through I, and which pass through J, where (O,I,J) is the base of the plane coordinate system?

   (a) $\{P(x,y):\ y = 3x\}$

   (b) $\{P(x,y):\ y = 3x + 1\}$

   (c) $\{P(x,y):\ y = x - 1\}$

   (d) $\{P(x,y):\ 58x + 69y = 0\}$

   (e) $\{P(x,y):\ x = 1\}$

   (f) $\{P(x,y):\ y = 1\}$

   (g) $\{P(x,y):\ y = -3x\}$

   (h) $\{P(x,y):\ x = 0\}$

7. For each pair of points given below, together with their O,I,J-coordinates, find an equation for the line that

contains them.

(a) A(3,0), B(5,0)
(b) C(4,2), D(2,0)
(c) E(4,2), F(2,4)
(d) G(-3,3), H(3,-3)
(e) K(6,2), L$(0,\frac{1}{2})$
(f) M(12,-2), N(6,10)
(g) P(4,-1), Q(8,1)
(h) R(0,5), S(-3,0)

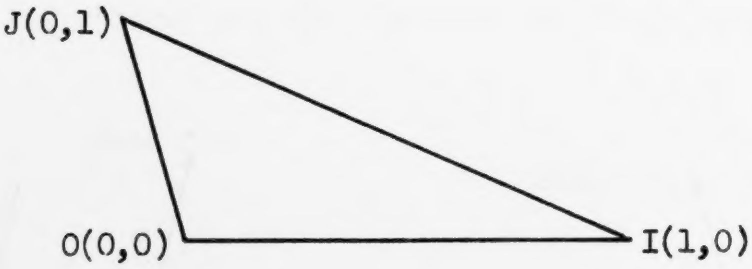
8. Find an equation for each of the following:

(a) $\overleftrightarrow{OI}$ (b) $\overleftrightarrow{OJ}$ (c) $\overleftrightarrow{IJ}$

9. Using set notation describe each of the following segments:

(a) $\overline{OI}$ (b) $\overline{OJ}$ (c) $\overline{IJ}$

10. What are the coordinates of the midpoint of $\overline{OI}$? of $\overline{OJ}$? of $\overline{IJ}$?



11. Find the coordinates of the midpoint of $\overline{AB}$, if A and B have coordinates listed below.

(a) A(0,2), B(4,0)
(b) A(2,3), B(6,1)
(c) A(-2,3), B(0,5)
(d) A(-2,-3), B(6,-2)
(e) A(-2,3), B(2,-3)
(f) A$(4,\frac{1}{2})$, B$(\frac{1}{2},-4)$

6.14 Intersections of Lines

Knowing equations for lines, it is a simple matter to determine the coordinates of their point of intersection, if any. The simplest case concerns two lines, one having an equation such as x = -1 the other having an equation such as

$y = 2$. Their intersection consists of a single point whose coordinates are $(-1,2)$. This is readily seen in Figure 6.20. For another case, let us take one line not parallel to either axis, and the other parallel to one of the axes. For example, let the first of these lines have equation $2x + 3y = 6$, and let the second have equation $x = 2$. (See Figure 6.21.) If they intersect, they must intersect in a point whose x-coordinate is 2. Using this information, we can get the y-coordinate of the point of intersection by replacing x with 2 in the first equation. This yields $2 \cdot 2 + 3y = 6$, from which we find $y = \frac{2}{3}$. Since $(2,\frac{2}{3})$ satisfies both equations, the point with these coordinates lies on both lines. It is point B.

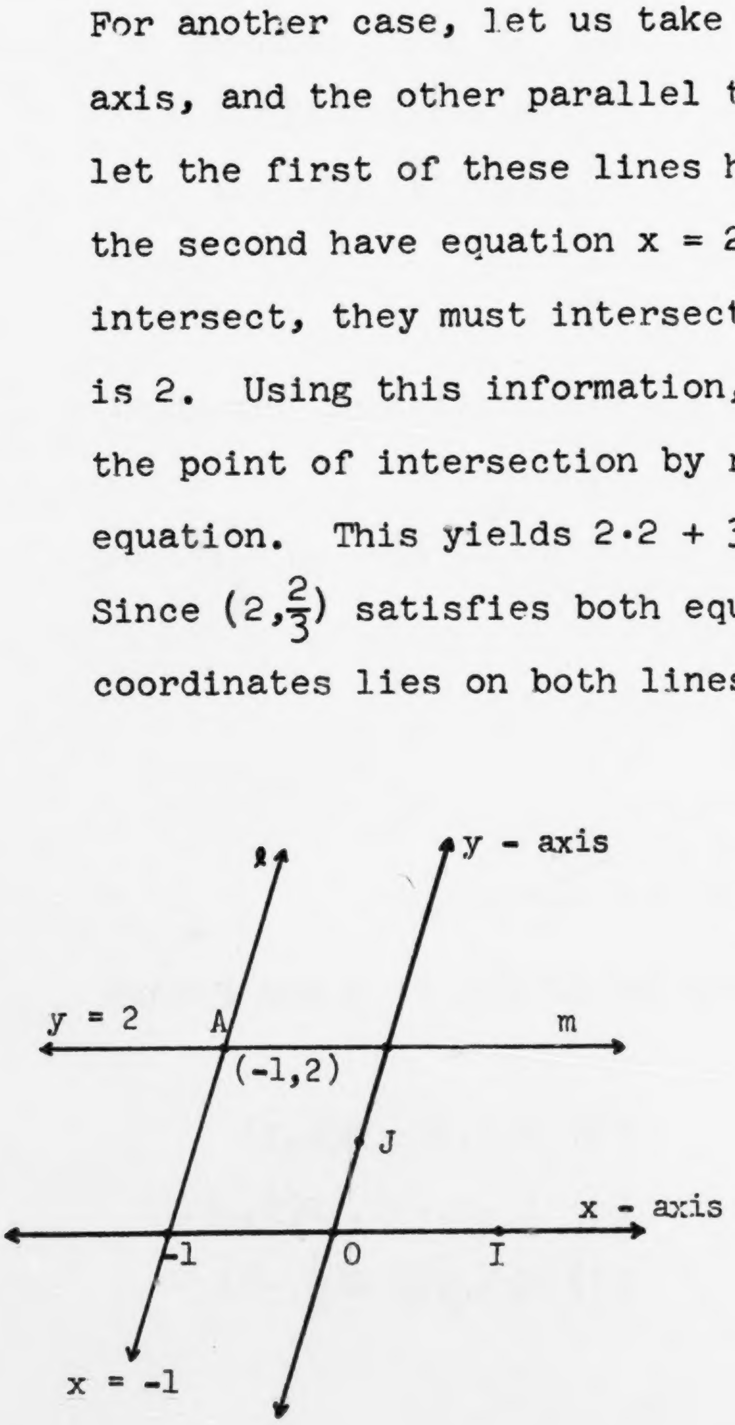


Figure 6.20

$\ell = \{P(x,y): x = -1\}$

$m = \{Q(x,y): y = 2\}$

$\ell \cap m = \{A(-1,2)\}$

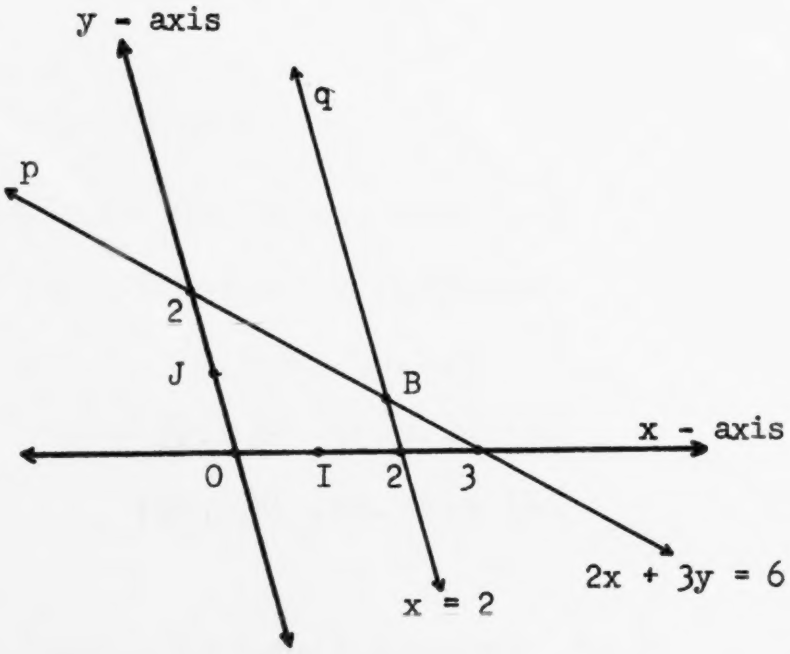


Figure 6.21

$p = \{P(x,y): 2x + 3y = 6\}$

$q = \{Q(x,y): x = 2\}$

$p \cap q = \{B(2,\frac{2}{3})\}$

Finally consider the case of two lines, neither of which is parallel to either axis. Let the first, for instance, have equation $2x + 3y - 5 = 0$ and let the second have equation $x + 2y - 3 = 0$. Such equations always have equivalent equations of the form $y = ax + b$. (Why?). Study the process by which these forms are found for each equation, as carried out below.

$2x + 3y - 5 = 0$	$x + 2y - 3 = 0$
$3y = -2x + 5$	$2y = -x + 3$
$y = -\frac{2}{3}x + \frac{5}{3}$	$y = -\frac{1}{2}x + \frac{3}{2}$

Assuming that the lines intersect, the point of intersection can have only one y-coordinate. The value of x for which this is true must therefore satisfy the condition

$$-\frac{2}{3}x + \frac{5}{3} = -\frac{1}{2}x + \frac{3}{2} ,$$

or

$$-4x + 10 = -3x + 9 ,$$

or

$$1 = x, \text{ and } y = -\frac{2}{3}\cdot 1 + \frac{5}{3} \text{ or } 1.$$

Therefore the intersection of the two lines is $\{P(1,1)\}$.

Check to see whether $(1,1)$ satisfies both $2x + 3y - 5 = 0$ and $x + 2y - 3 = 0$.

Our discussion would not be complete without considering a pair of lines that do not intersect, for instance lines with equations $y = 8x + 2$ and $y = 8x - 4$. If we assume that they do intersect, in an attempt to find the point of intersection, we would have to solve

$$8x + 2 = 8x - 4.$$

Does this equation have a solution?

In general two lines ℓ and m are parallel if they have equations of the form (1) $x = a$ and $x = b$, or (2) $y = a$ and $y = b$, or (3) $y = ax + b$ and $y = ax + c$. In each case, if ℓ and m are distinct lines with the equations specified, then $\ell \cap m = \emptyset$.

6.15 Exercises

Assume an (O,I,J) coordinate system in these exercises.

1. For each pair of lines listed below, find the coordinates of their point of intersection, if any.
   (a) $\{P(x,y)\colon x = 8\}$ and $\{P(x,y)\colon y = 3\}$
   (b) $\{P(x,y)\colon x = -2\}$ and $\{P(x,y)\colon x = 2\}$
   (c) $\{P(x,y)\colon x = 2\}$ and $\{P(x,y)\colon x + y = 8\}$
   (d) $\{P(x,y)\colon y = 3\}$ and $\{P(x,y)\colon 4x = 3\}$
   (e) $\{P(x,y)\colon y = 3 - x\}$ and $\{P(x,y)\colon y = x - 3\}$
   (f) $\{P(x,y)\colon x + y = 7\}$ and $\{P(x,y)\colon 2x - y = 2\}$
   (g) $\{P(x,y)\colon x - y = 7\}$ and $\{P(x,y)\colon 4x - 2 = y\}$
   (h) $\{P(x,y)\colon 2x - 3y = 4\}$ and $\{P(x,y)\colon 6y = 4x + 8\}$

2. Let A have coordinates (2,2). Find the coordinates of the point of intersection, if any, of
   (a) $\overleftrightarrow{OA}$ and $\overleftrightarrow{IJ}$.   (b) $\overleftrightarrow{JA}$ and $\overleftrightarrow{OI}$.
   (c) $\overleftrightarrow{IA}$ and $\overleftrightarrow{OJ}$.

3. Determine whether or not $A(3,2)$, $B(1,1)$ and $C(-3,-1)$ are on one line. (Hint: Use an equation for $\overleftrightarrow{AB}$.)

4. Determine whether or not the triple of points in each part listed below is a collinear set.
   (a) $A(0,-5)$, $B(3,1)$, $C(-2,-9)$.

(b) $D(2,4)$, $E(0,8)$, $F(3,1)$.

(c) $K(0,0)$, $L(12,12)$, $M(-1,-1)$.

(d) $P(a,-b)$, $Q(0,0)$, $R(-a,b)$, where $a \neq 0$, $b \neq 0$.

5. (a) Copy the table below and fill in your copy, given that the point with coordinates (x,y) lies on the line with equation $y = 2x - 3$.

x	-1	0	1	2	3
y				1	3

Calculate the value of $\frac{y_2 - y_1}{x_2 - x_1}$ when $(x_1, y_1) = (2,1)$ (that is: $x_1 = 2$, $y_1 = 1$), and $(x_2, y_2) = (3,3)$. Calculate the value of $\frac{y_2 - y_1}{x_2 - x_1}$ for any two pairs of coordinates in your table, if (x_1, y_1) is one pair, and (x_2, y_2) is the other. Are the results the same? Are they equal to 2, the coefficient of x in the equation?

(b) If $x_1 = p$, then $y_1 = 2p - 3$. If $x_2 = q$, then $y_2 = 2q - 3$. Find the value of $\frac{y_2 - y_1}{x_2 - x_1}$ for these values of (x_1, y_1) and (x_2, y_2). Is the result still equal to 2? Complete the statement which this proves: If (x_1, y_1) and (x_2, y_2) are coordinate of any two points of line ℓ with equation $y = 2x - 3$, then ...

(c) Prove the statement: If (x_1, y_1) and (x_2, y_2) are coordinates of any two points on ℓ with equation $y = ax + b$, then $\frac{y_2 - y_1}{x_2 - x_1} = a$. The value of a is called the O,I,J-slope of the line. If a line has no equation of the form $y = ax + b$, we say that the line has no slope. Thus the line with equation $x = 3$ has no slope. But the slope of the line with equation

$y = 3$ is 0.

(d) For each equation listed below, what is the slope of the line for which it is an equation?

$y = 5x - 2, \quad y = -2x + 2, \quad y = 5, \quad Y = \frac{1}{2}x - 8.$

(e) Show that two lines with equations $y = ax + b$ and $y = ax + c$ are parallel.

6. Let line ℓ contain A(2,3) and B(4,7). We can find an equation for ℓ by using the fact that the slope of a line is independent of the choice of the two points used to calculate it. Thus if P(x,y) is any point of ℓ, other than A, we can claim, since $x - 2 \neq 0$

$$\frac{y - 3}{y - 2} = \frac{7 - 3}{4 - 2} \text{ or } 2,$$

and $$y - 3 = 2(x - 2).$$

Note that the last equation is satisfied by (2,3), as well as by the coordinates of all other points of ℓ. Hence it is an equation for ℓ. The form of this equation is called the point-slope form. What is an equation for m, if it contains C(6,2) and D(5,3)? (Hint: Calculate the slope and use the point-slope form directly with either (6,2) or (5,3).)

7. A line contains points A(1,-2) and B(3,-5).

(a) Find the slope of this line.

(b) Write an equation for the line.

(c) What is the y-coordinate of a point of this line if its x-coordinate is 20?

(d) What is the x-coordinate of a point of this line if its y-coordinate is 8?

8. Write two equations, one for a line with no slope, the other for a line with zero slope, if the lines intersect in point A(-2,3).

6.16 Triangles and Quadrilaterals

In this section you will see how the mathematical machinery now at our disposal can be used to prove statements about triangles and quadrilaterals. We start with the following definitions.

Definitions. Let A,B,C be three non-collinear points. Then $\overline{AB} \cup \overline{BC} \cup \overline{CA}$ is a triangle. It is denoted $\triangle ABC$. A median of a triangle is a segment that joins a vertex of the triangle to the midpoint of the side opposite that vertex. How many medians does a triangle have?

Theorem 5. The medians of a triangle meets in a point.

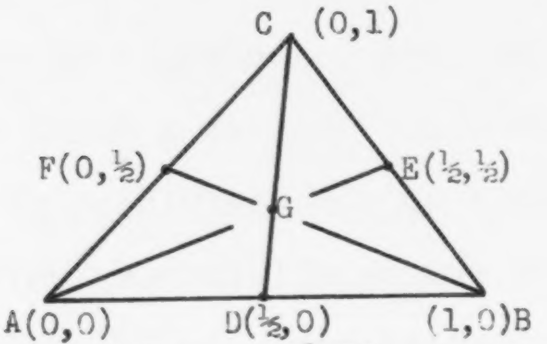


Figure 6.22

Proof. Let the vertices of the triangle be A, B, C (see Figure 6.22). Since points A, B, C are noncollinear, (A,B,C) may serve as the base of a plane coordinate system. The coordinates of D, the midpoint of $\overline{AB}$, are $(\frac{1}{2},0)$; the coordinates of F, the midpoint of $\overline{AC}$, are $(0,\frac{1}{2})$. Let E be the midpoint of $\overline{BC}$. Its x-coordinate is its C,B-coordinate, and its y-coordinate is its B,C-coordinate. Thus its A,B,C-coordinates are $(\frac{1}{2},\frac{1}{2})$.

An equation for $\overleftrightarrow{AE}$ is (1) $y - 0 = \dfrac{\frac{1}{2} - 0}{\frac{1}{2} - 0}(x - 0)$, or $y = x$.

An equation for $\overleftrightarrow{BF}$ is (2) $y - 0 = \dfrac{0 - \frac{1}{2}}{1 - 0}(x - 1)$, or $y = -\frac{1}{2}(x - 1)$.

An equation for $\overleftrightarrow{CD}$ is (3) $y - 1 = \dfrac{1 - 0}{0 - \frac{1}{2}}(x - 0)$, or $y - 1 = -2x$.

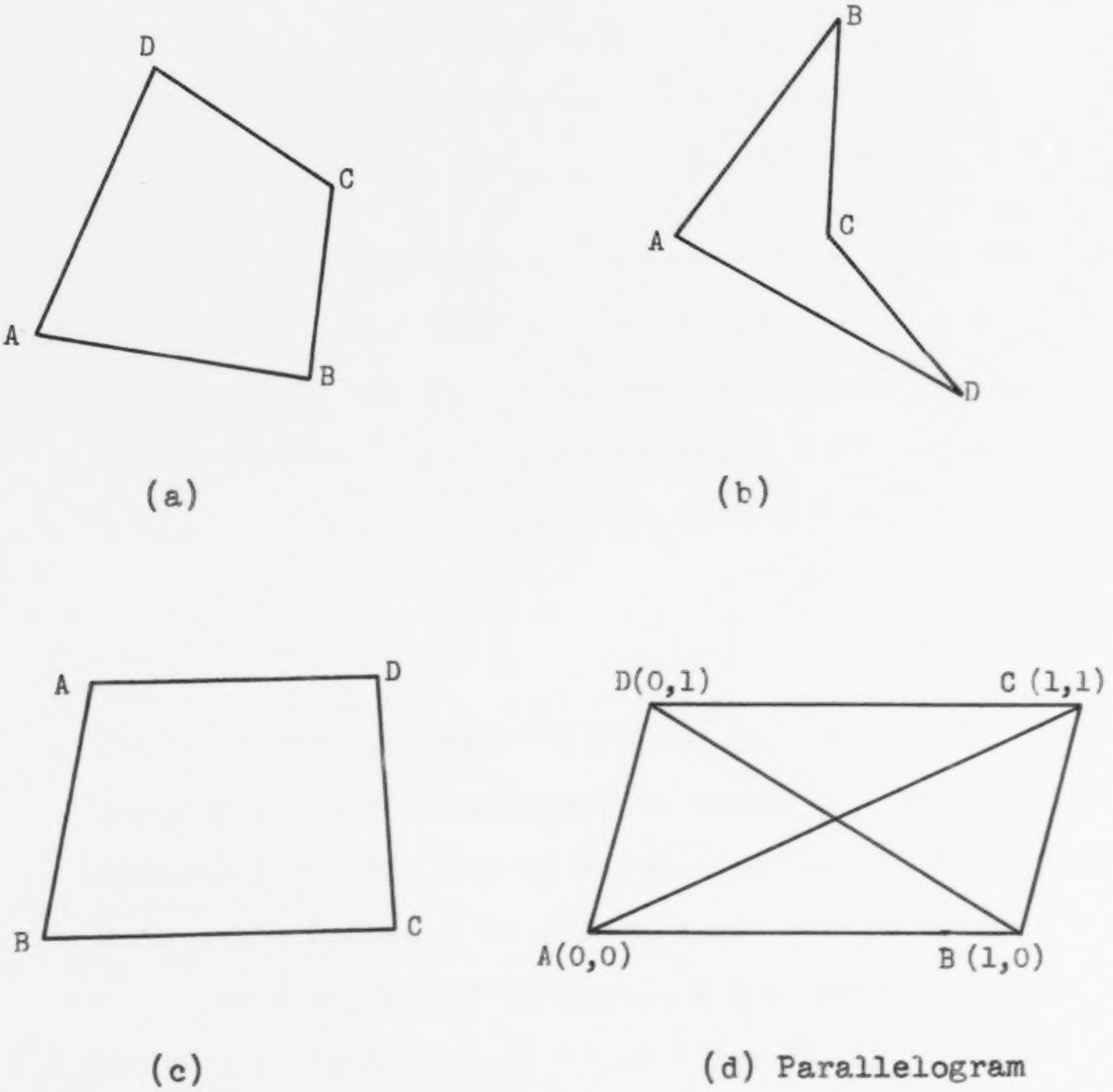
Solving equations (1) with (2) we get the solution $(\frac{1}{3},\frac{1}{3})$. Solving equations (1) with (3) we get the solution $(\frac{1}{3},\frac{1}{3})$. Solving equations (2) with (3) we still get the solution $(\frac{1}{3},\frac{1}{3})$. We conclude: $\overleftrightarrow{AE} \cap \overleftrightarrow{BF} = \overleftrightarrow{AE} \cap \overleftrightarrow{CD} = \overleftrightarrow{BF} \cap \overleftrightarrow{CD}$, and the theorem is proved. Let us call the point in which the medians meet G. Furthermore we see, by studying, say only x-coordinates of points in $\overline{AE}$ that G divides $\overline{AE}$, from A to E, in the ratio 2:3. In fact G divides every median, from vertex to opposite midpoint in the ratio 2:3. This is a bonus we did not expect.

As a second example of the usefulness of coordinates, we prove a theorem about any parallelogram, which you know is a special case of a quadrilateral.

Definition. Let A, B, C, D be four points of a plane such that no three are collinear, $\overline{AB} \cap \overline{CD} = \emptyset$ and $\overline{BC} \cap \overline{AD} = \emptyset$. Then $\overline{AB} \cup \overline{BC} \cup \overline{CD} \cup \overline{DA}$ is a quadrilateral. It is named ABCD, BCDA, CDAB, DABC, DCBA, CBAD, BADC, or ADCB. The diagonals of this quadrilateral are $\overline{AC}$ and $\overline{BD}$.

Note: In each name of the quadrilateral, a cyclic order of the vertices is kept. ABDC, for example, does not name the same quadrilateral. (See Figure 6.23.)

Definition. A quadrilateral ABCD is called a parallelogram if $\overleftrightarrow{AB} \parallel \overleftrightarrow{DC}$ and $\overleftrightarrow{AD} \parallel \overleftrightarrow{BC}$. (See Figure 6.23 (d).)



(a)

(b)

(c)

(d) Parallelogram

Figure 6.23

Some Pictures of Quadrilateral ABCD

Theorem 6. The diagonals of a parallelogram bisect each other (See Figure 6.23 (d).)

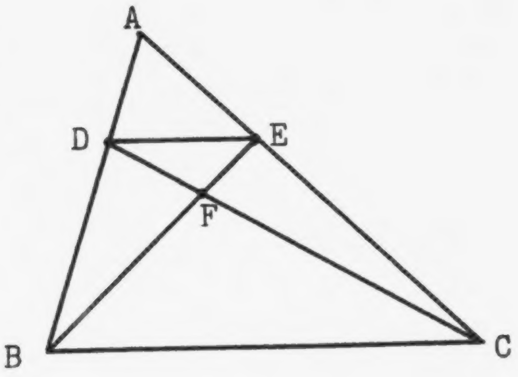
Proof. The A,B,D-coordinates of A, B, and D are (0,0), (1,0) and (0,1) respectively. Since C is on the parallel to $\overleftrightarrow{AD}$ that passes through B, its x-coordinate is 1. Since C is on the parallel to $\overleftrightarrow{AB}$ that passes through D, its y-coordinate is 1. An equation for $\overleftrightarrow{AC}$ is (1) $y = x$. An equation for $\overleftrightarrow{BD}$ is (2) $x + y = 1$. Solving (1) with (2) gives the solution set $\{(\frac{1}{2},\frac{1}{2})\}$.

We conclude that the diagonals bisect each other. Explain why.

Note in both proofs we chose a base for a plane coordinate system that was convenient for our purposes. In doing the exercises that follow you should also try to choose a base that is convenient for your purposes.

6.17 Exercises

1. Prove: The line that passes through the midpoints of two sides of a triangle is parallel to the third side.
2. Prove: If a line is parallel to one side of a triangle and passes through the midpoint of a second side, then it passes through the midpoint of the third side.
3. In $\triangle ABC$, D is in $\overline{AB}$ and E is in $\overline{AC}$ such that BD : DA = 2 : 1, and CE : EA = 2 : 1.



(a) Prove: $\overleftrightarrow{DE} \parallel \overleftrightarrow{BC}$.

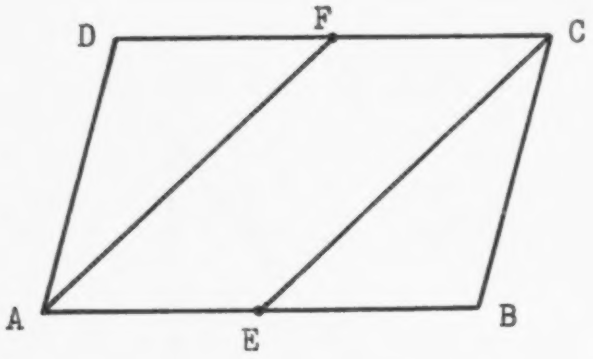
(b) Let $\overline{BE} \cap \overline{CD} = \{F\}$.

Show $BF : FE = CF : FD = 3 : 1$.

4. Prove: ABCD is a parallelogram if the A,B,D-coordinate of C is (1,1).

5. Prove: Quadrilateral ABCD is a parallelogram if $\overline{AC}$ and $\overline{BD}$ bisect each other.

6. Prove: Let ABCD be a parallelogram; let E be the midpoint of $\overline{AB}$, and F the midpoint of $\overline{DC}$. Prove AECF is a parallelogram. (Hint: Using slopes show $\overleftrightarrow{AF} \parallel \overleftrightarrow{EC}$.)



7. Using the data in Exercise 6 show that if $\overline{AF} \cap \overline{DB} = \{G\}$, Then G divides $\overline{AF}$, from A to F, in the ratio 2:3.

8. In quadrilateral ABCD let the midpoints of $\overline{AB}$, $\overline{BC}$, $\overline{CD}$

and $\overline{DA}$ be E, F, G, and H respectively. Prove that EFGH, if it forms a quadrilateral, is a parallelogram.

6.18 The Pythagorean Property

So far in this chapter we have made no references to perpendicular lines (see Course I, Sections 9.6 and 10.13), nor have we compared lengths of segments on different lines. In spite of this we have managed to develop a considerable body of geometry. But there are relations in geometry that do use perpendicular lines and do compare lengths of segments on different lines. This is done for instance in a statement about right triangles named after a famous Greek mathematician Pythagoras (c. 580 - 500 B.C.).

In Figure 6.24, assume that $\overleftrightarrow{BC}$ is perpendicular to $\overleftrightarrow{AC}$ (written $\overleftrightarrow{BC} \perp \overleftrightarrow{AC}$). Then $\triangle ABC$ is a right triangle, $\angle BCA$ is a right angle, $\overline{AC}$ and $\overline{BC}$, the sides that lie in the perpendicular lines, are called legs of the triangle and $\overline{AB}$ is called the hypotenuse of the right triangle.

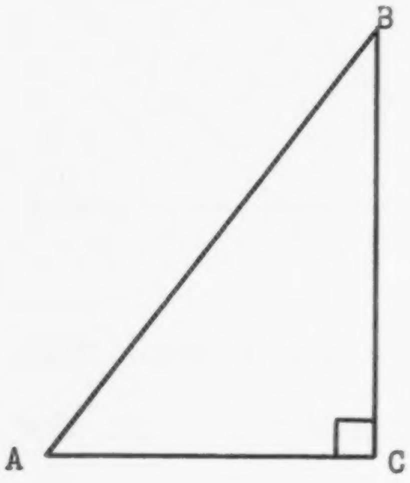


Figure 6.24

If the length of $\overline{BC}$ is a, the length of $\overline{AC}$ is b, and the length of $\overline{AB}$ is c, then the Pythagorean property of right triangles is given by the equation

$$a^2 + b^2 = c^2.$$

If you like you can measure the lengths of the three sides of a right triangle, square each length and see if the equation is approximately true. But we present another approach which is based on the idea that if the side of a square has length s, then the area of the square is s^2.

We start with a right triangle as shown in Figure 6.25, whose legs have lengths a and b and whose hypotenuse has length c.

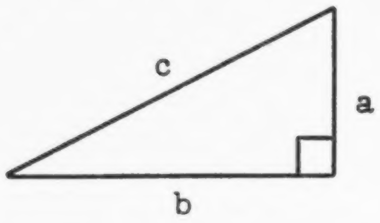


Figure 6.25

We can arrange four copies of this triangle to form a square as shown in Figure 6.26, or Figure 6.27.

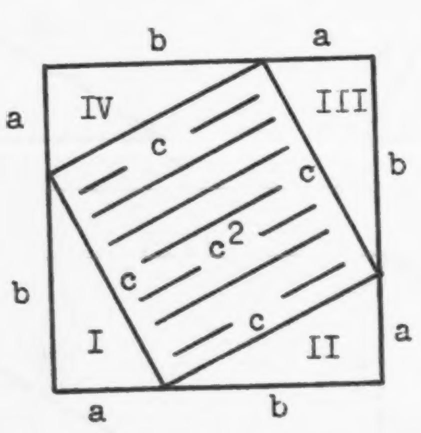


Figure 6.26

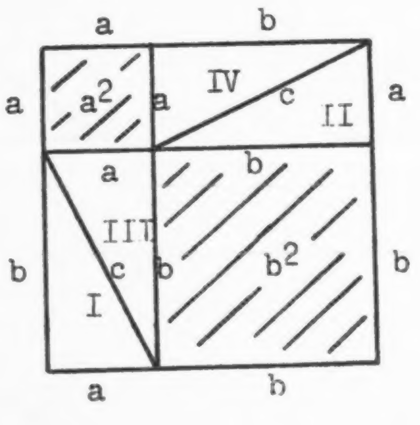


Figure 6.27

What is the area of the large square in each diagram? In Figure 6.26 the shaded region is the uncovered part of the large square after setting the four triangles in position. What is its area? In Figure 6.27 two shaded regions are the uncovered parts of the large square. What is the sum of their areas? But no matter how the four triangles are positioned within the large square, as long as they do not overlap, the uncovered region should have the same area. Therefore

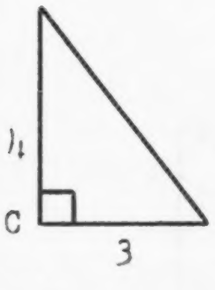
$$c^2 = a^2 + b^2.$$

We have not deduced this from statements in our system, and hence we cannot call it a theorem. In recognition of this, let us call it the Pythagorean property of right triangles, and you may regard it as an axiom hereafter in our system.

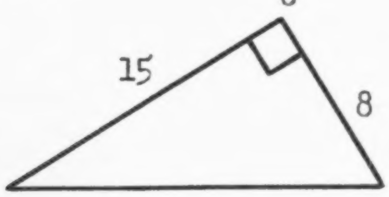
6.19 Exercises

1. In each of the following right triangles, ∠C is the right angle, and the lengths of two sides are indicated in terms of the same unit. Find the length of the third side.

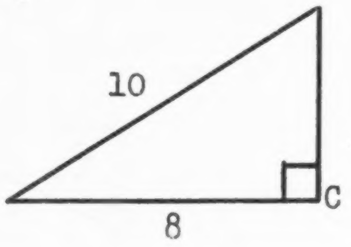
(a)



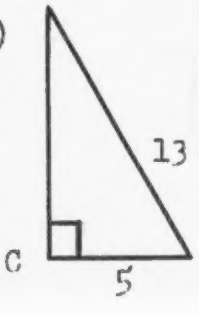
(b)



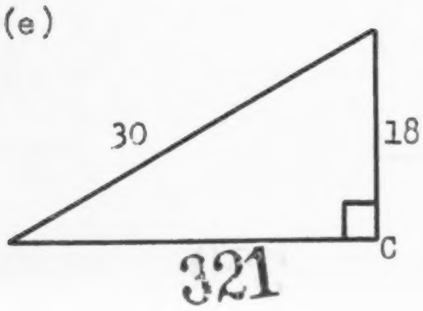
(c)



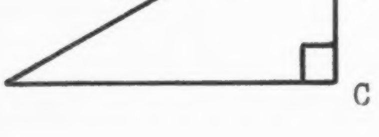
(d)



(e)

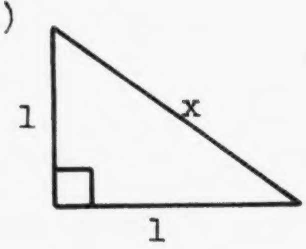


(f)

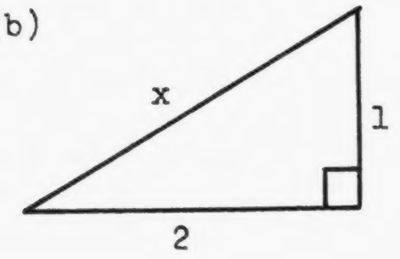


2. Find x in each of the following right triangles. If it is irrational, leave it in radical form.

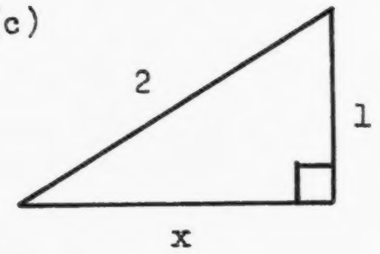
(a)



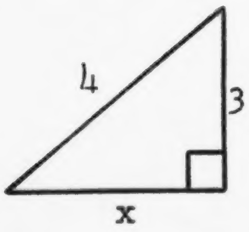
(b)



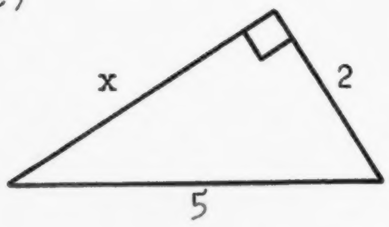
(c)



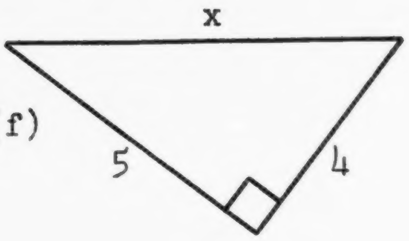
(d)



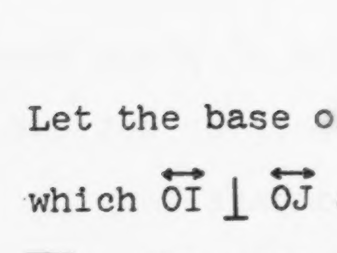
(e)



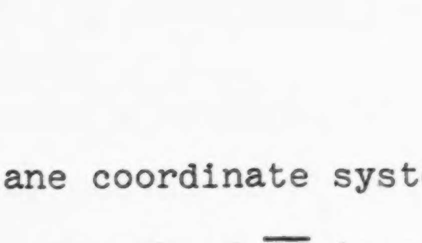
(f)



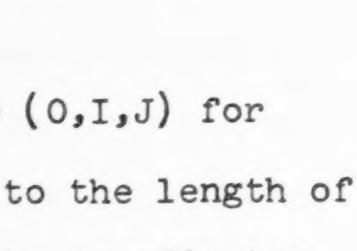
(g)



(h)



(i)

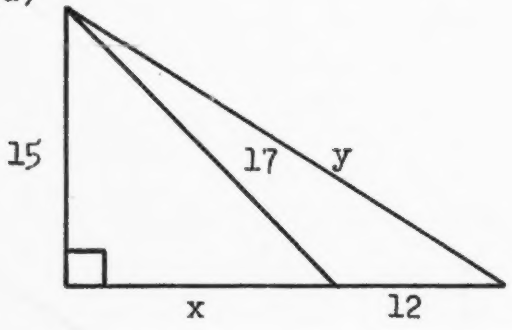

$\sqrt{26}$
x
$\sqrt{23}$

3. Let the base of a plane coordinate system be (0,I,J) for which $\overleftrightarrow{OI} \perp \overleftrightarrow{OJ}$ and the length of $\overline{OI}$ is equal to the length of $\overline{OJ}$. Find the length of $\overline{AB}$ if A and B have the coordinates listed below. Leave irrational answers in radical form.

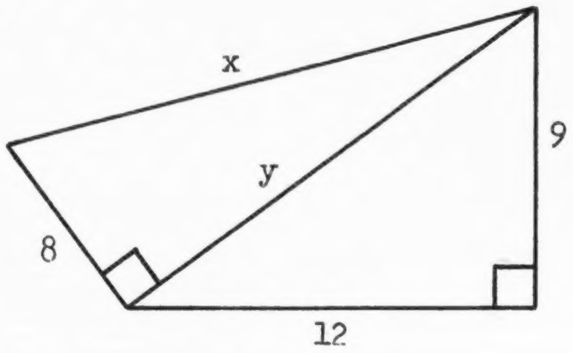
(a) A(4,0), B(3,0)
(b) A(-4,0), B(3,0)
(c) A(5,0), B(12,0)
(d) A(2,0), B(0,-2)
(e) A(7,0), B(0,-3)
(f) A(0,-2), B(-1,0)

4. Using the coordinate system in Exercise 3, find the coordinates of A, a point in the positive y-axis if
   (a) AB = 10 and B has coordinates (6,0).
   (b) AB = 13 and B has coordinates (12,0).
   (c) AB = 4 and B has coordinates $(-2\sqrt{2},0)$.
   (d) AB = 12 and B has coordinates (-6,0).
5. In each figure below are two right triangles. Find x and y in each. Right angles are marked by a square corner.

(a)



(b)



6.20 Plane Rectangular Coordinate Systems

We are ready now to consider a special kind of plane coordinate system that enables us to investigate whether or not two lines in the plane are perpendicular, and to compare lengths of segments on different lines. Figure 6.28 shows such a system. Note that the axes are perpendicular to each other, and the length of $\overline{OI}$ is equal to the length of $\overline{OJ}$.

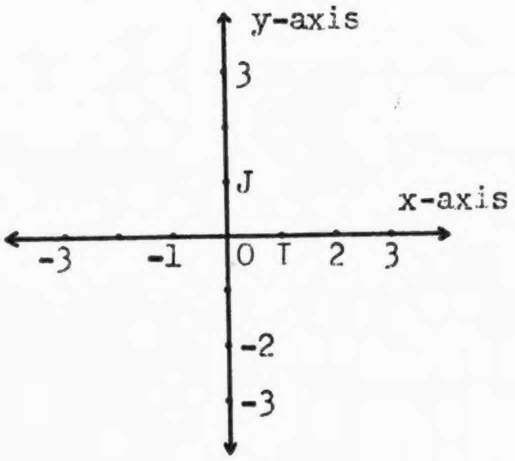


Figure 6.28

Definition. A plane coordinate system with base (O,I,J) is called rectangular if $\overleftrightarrow{OI} \perp \overleftrightarrow{OJ}$ and $OI = OJ = 1$.

The coordinate formulas we used for midpoints and slopes continue to be operative for rectangular coordinate systems, and we continue to describe lines by equations of the form $ax + by + c = 0$. Rectangular coordinate systems have the added advantage over other systems in that we can study perpendicularity of lines, and we can compare distances on different lines. To compute these distances we use the distance formula given below. Note that we call the coordinates rectangular. This means we are using a rectangular coordinate system.

If P_1 and P_2 have rectangular coordinates (x_1, y_1) and (x_2, y_2) respectively, then the length of $\overline{P_1P_2}$ is

$$P_1P_2 = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}\ .$$

We consider four cases:

Case 1. $P_1 = P_2$. (For other cases $P_1 \neq P_2$.)

Case 2. $\overleftrightarrow{P_1P_2} \parallel \overleftrightarrow{OI}$.

Case 3. $\overleftrightarrow{P_1P_2} \parallel \overleftrightarrow{OJ}$.

Case 4. $\overleftrightarrow{P_1P_2}$ is not parallel to either $\overleftrightarrow{OI}$ or $\overleftrightarrow{OJ}$.

Case 1. If $P_1 = P_2$, then $x_1 = x_2$ and y_1 and y_2. The formula to be proved then takes the form

$$\sqrt{(x_1 - x_1)^2 + (y_1 - y_1)^2} = \sqrt{0^2 + 0^2} = 0.$$

This is exactly what the distance should be, so the formula works when $P_1 = P_2$.

Case 2. (See Figure 6.29.) Since $\overleftrightarrow{P_1P_2} \parallel \overleftrightarrow{OI}$, $y_1 = y_2$. Then $y_1 - y_2 = 0$ and the formula becomes

$$\sqrt{(x_1 - x_2)^2 + 0^2} = |x_1 - x_2|.$$

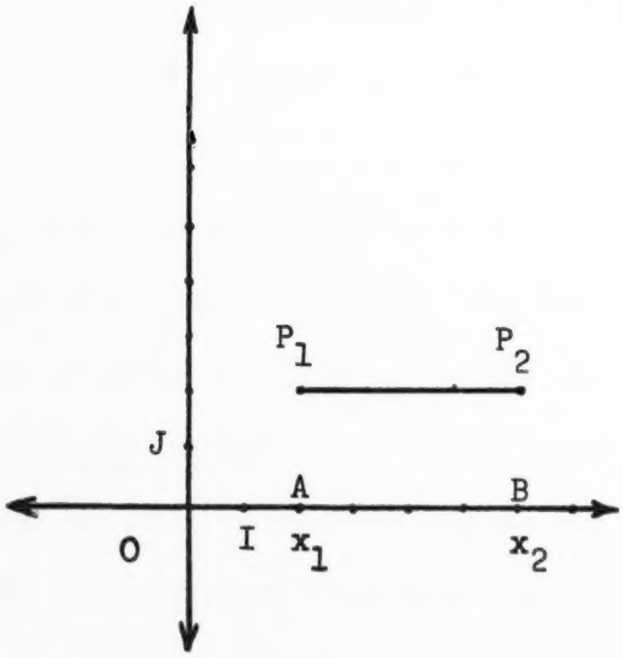


Figure 6.29

The parallels to $\overleftrightarrow{OJ}$ through P_1 and P_2 intersect $\overleftrightarrow{OI}$ in two points, A and B whose O,I-coordinates are x_1 and x_2. So $AB = |x_1 - x_2|$.

It is reasonable to assume (we do not prove) that the O,I-length of $\overline{P_1P_2}$ is also $|x_1 - x_2|$. If we do, then the formula works for Case 2.

Case 3. By a similar argument it works for Case 3.

Case 4. For this case $x_1 \neq x_2$ and $y_1 \neq y_2$, see Figure 6.30. Take point A with coordinates (x_2, y_1). Since the x-coordinates of P_2 and A are the same, $\overleftrightarrow{AP_2} \parallel \overleftrightarrow{OJ}$.

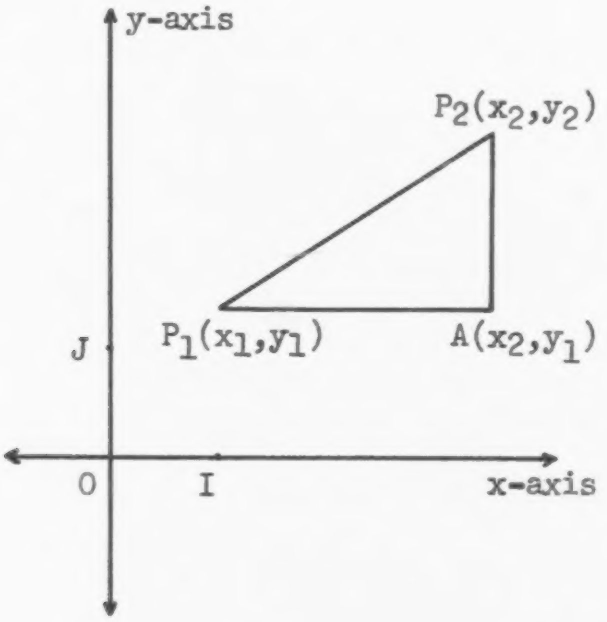


Figure 6.30

Since the y-coordinate of P_1 and A are the same, $\overleftrightarrow{AP_1} \parallel \overleftrightarrow{OI}$. We assume that every line parallel to $\overleftrightarrow{OJ}$ is perpendicular to every line parallel to $\overleftrightarrow{OI}$. So ΔP_1AP_2 is a right triangle, with right angle at A. Thus the Pythagorean property is available and we have

(1) $(P_1P_2)^2 = (AP_1)^2 + (AP_2)^2$.

By the preceding cases $(AP_1)^2 = (x_1 - x_2)^2$ and $(AP_2)^2 = (y_1 - y_2)^2$. Making these substitutions for $(AP_1)^2$ and $(AP_2)^2$ in (1) and taking the square root of each member yields the desired result.

6.21 Exercises

1. Find the distance between each pair of points listed below if the coordinates given are rectangular coordinates.
   (a) A(0,0), B(3,4)
   (b) C(2,1), D(-2,4)
   (c) E(3,2), F(3,7)
   (d) P(4,-2), Q(8,-2)
   (e) R(6,1), S(0,-1)
   (f) T(4,3), V(4,3)
   (g) A(1,-3), B(-4,7)
   (h) C(2,0), D(0,-3)
   (i) E(a,0), F(0,b)
   (j) G(a,b), H(a,c)
   (k) K(a,b), L(c,b)
   (l) M(a,b), N(c,d)
2. The vertices of $\triangle ABC$ are listed below with rectangular coordinates. For each triangle show that two of its sides have equal lengths.
   (a) A(-1,3), B(5,-1), C(9,5)
   (b) A(1,-1), B(-4,4), C(3,5)
   (c) A(3,5), B(1,-3), C(-6,3)
   (d) A(5,0), B(3,4), C(1,0)
   (e) A(0,2), B(3,1), C(1,-1)
3. ABCD is a rectangle, which by definition is a parallelogram that has at least one right angle. If in a rectangular coordinate system A has coordinates (0,0), B has coordinates (3,0) and D has coordinates (0,4), what coordinates should C have? Using the distance formula show that the diagonals $\overline{AC}$ and $\overline{BD}$ have the same length.
4. (a) Assume rectangular coordinates for the vertices of $\triangle ABC$

to be as follows: C(0,0), B(6,0), A(0,8). Find the coordinates of the midpoint of $\overline{AB}$ and show that the length of the median from C is one-half the length of $\overline{AB}$.

(b) Repeat for C(0,0), B(12,0), A(0,5).

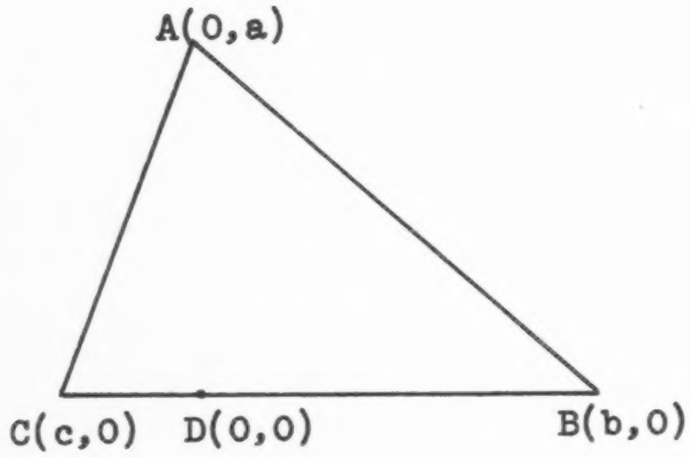
(c) Repeat for C(0,0), B(a,0), A(0,b).

(d) Complete the sentence which seems indicated by these results: The length of the median to the hypotenuse of a right triangle is ...

5. Assume rectangular coordinates for the vertices of $\triangle ABC$ to be as follows: A(4,0), B(0,6), C(-4,0). Find the coordinates of the midpoints of $\overline{AB}$ and $\overline{BC}$. Show that the length of the median from A is equal to the length of the median from C.

6. Show that ABCD is a parallelogram if A, B, C, D have rectangular coordinates (0,0), (3,2), (7,6), (4,4) respectively. Then show that AB = CD and BC = DA.

7. Suppose for $\triangle ABC$, $(AB)^2 = (AC)^2 + (BC)^2$. As you recall, this is the equation that is a property of right triangles. In this exercise we investigate whether or not a triangle that has this property is necessarily a right triangle. If so, which of the three sides, $\overline{AB}$, $\overline{BC}$, or $\overline{CA}$, would you expect to be the hypotenuse? To begin this investigation, let us consider the line through A that is perpendicular to $\overleftrightarrow{CB}$, and let it intersect $\overleftrightarrow{CB}$ in D.



If C = D, there is nothing left to prove. Suppose then $C \neq D$. Using the perpendiculars $\overleftrightarrow{CB}$ and $\overleftrightarrow{AD}$ as axes we set up a rectangular coordinate system. In this system D has coordinates (0,0). Let A,B,C have respective coordinates (0,a), (b,0) and (c,0). By the distance formula

$$(AB)^2 = (b - 0)^2 + (0 - a)^2 = b^2 + a^2,$$
$$(AC)^2 = (c - 0)^2 + (0 - a)^2 = c^2 + a^2$$
$$(BC)^2 = (c - b)^2 + (0 - 0)^2 = c^2 - 2cb + b^2.$$

Using the equation $(AB)^2 = (AC)^2 + (BC)^2$, the given information, show $c = 0$. What conclusion does this allow you to make?

8. The three numbers in each part of this exercise are lengths of sides of a triangle. Identify those that are lengths of sides of right triangles, and for these, identify the hypotenuse.

(a) 15, 20, 25 (b) 24, 25, 7 (c) $\sqrt{3}, \sqrt{4}, \sqrt{7}$
(d) $\sqrt{3}, \sqrt{3}, 3$ (e) 4, 5, 6 (f) $2, 2\sqrt{3}, 4$
(g) $3\sqrt{2}, 3\sqrt{3}, 3\sqrt{4}$ (h) 40, 9, 41 (i) 3a, 4a, 5a $(a > 0)$

6.22 Summary

This chapter continues the development of the axiomatic system begun in Chapter 3. This was done by adding three axioms concerning coordinate systems on lines.

Axiom 4 states that for each base (O,I) on a line there is exactly one coordinate system.

Axiom 5 asserts that if two coordinate systems are introduced on a line, then their respective coordinates $\underline{x}$ and $\underline{x'}$ are related by a rule of the form $x' = ax + b$ $(a \neq 0)$ of an affine transformation; that is, a dilation followed by a translation.

Axiom 6 describes a property of a parallel projection from one line to another. If A and B are points of the first line and A' and B' are their respective images under a parallel projection, then for every point X of the first line, the A',B'-coordinate of its image X' is the same as the A,B-coordinate of X.

These axioms enabled us to use numbers to express relations among geometric objects. This was done in the following definitions: The betweeness relation for points, line segment, ray, midpoint of a segment, and the ratio in which a point divides a segment.

The six axioms enabled us to construct a plane coordinate system which was determined by a choice of a base (O,I,J). Because of the one-to-one correspondence between the set of points in the plane and the set of ordered pairs of real numbers in each plane coordinate system, we are able to describe a set of points precisely by describing relationships of coordinates of the points in the set. We did this with equations and inequalities for lines, segments, rays and regions.

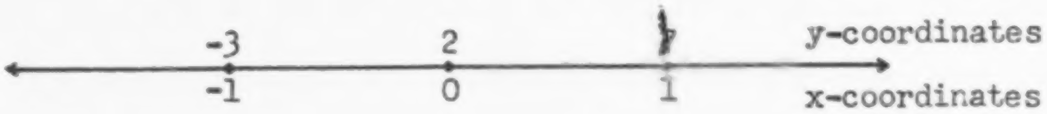
Of particular importance was the theorem that an equation of the form ax + by + c = 0 (where a and b are not both zero), can be used to describe any line in the plane. This opened the door for investigating lines by working with their equations. We did this in investigating triangles and parallelograms.

After accepting informally the notion of perpendicular lines and the Pythagorean property of right triangles (and some other properties), we were able to describe a plane rectangular coordinate system. This system has the virtue, not possessed by other coordinate systems, of enabling us to compare lengths of segments on different lines. This is done by the distance formula. Also we can establish whether or not a given triangle is a right triangle by using the converse of the Pythagorean property.

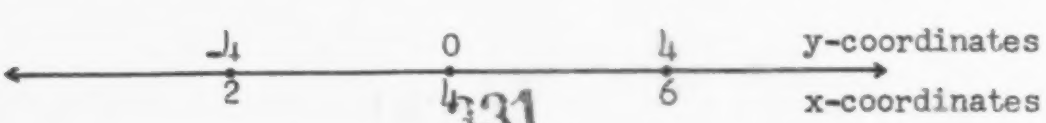
6.23 Review Exercises

1. Using the data indicated in the figures below, which show two coordinate systems on a line, find the formula that converts x-coordinates to y-coordinates.

(a)

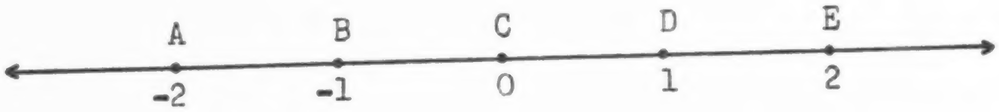


(b)



2. Using the data in Exercise 1, find the formula for each part that converts y-coordinates to x-coordinates.

3. Using set notation, and letting x̲ represent C,D-coordinates, describe each of the sets of points designated below as it applies to the figure below.



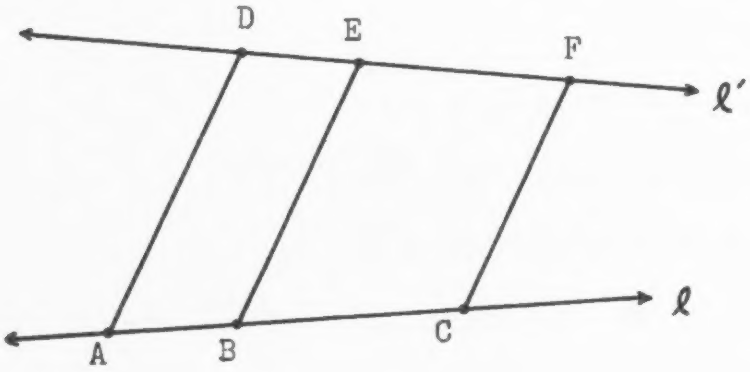
(a) $\overline{AD}$ (b) $\overrightarrow{AD}$ (c) $\overrightarrow{DA}$ (d) $\overleftrightarrow{AD}$

(e) $\overline{AD} \cap \overline{BC}$ (f) $\overline{AB} \cup \overline{BC}$ (g) $\overline{AC} \cup \overrightarrow{BD}$

(h) $\overline{AC} \cap \overline{CD}$ (i) $\overline{AB} \cap \overline{CD}$ (j) the midpoint of $\overline{BE}$

(k) the point that divides $\overline{AE}$, from A to E, in the ratio of 3:4.

4. Let f be a parallel projection from line ℓ to line ℓ' and let A, B, C be distinct points on ℓ. Furthermore let $A \xrightarrow{f} D$, $B \xrightarrow{f} E$ and $C \xrightarrow{f} F$.



Show that B divides $\overline{AC}$, from A to C, in the same ratio as E divides $\overline{DF}$ from D to F. Also show that C divides $\overline{BA}$, from B to A, in the same ratio as F divides $\overline{ED}$ from E to D.

5. Using a plane coordinate system of your choice make a graph

of each of the following sets of points. Use a different coordinate system for each part.

(a) $\{P(x,y): y = 3, -2 \leq x \leq 1\}$

(b) $\{P(x,y): y = 1, x \geq 1\}$

(c) $\{P(x,y): x = 3\}$

(d) $\{P(x,y): y = x \text{ and } -1 \leq x \leq 1\}$

(e) $\{P(x,y): y = 3x - 1 \text{ and } -1 \leq y \leq 2\}$

(f) $\{P(x,y): x + 2y - 2 = 0\}$

(g) $\{P(x,y): 2x - 3y - 6 = 0\}$

(h) $\{P(x,y): -2 \leq x < 2 \text{ and } -2 < y < 2\}$

6. For each pair of points listed below, with coordinates in a certain plane coordinate system, find an equation for the line that contains the points in each pair.

(a) $A(3,2)$, $B(8,2)$
(b) $C(-2,4)$, $D(-2,-4)$
(c) $D(3,3)$, $E(-3,-3)$
(d) $F(3,-3)$, $G(-3,3)$
(e) $G(0,2)$, $H(3,0)$
(f) $K(-2,3)$, $L(0,-2)$

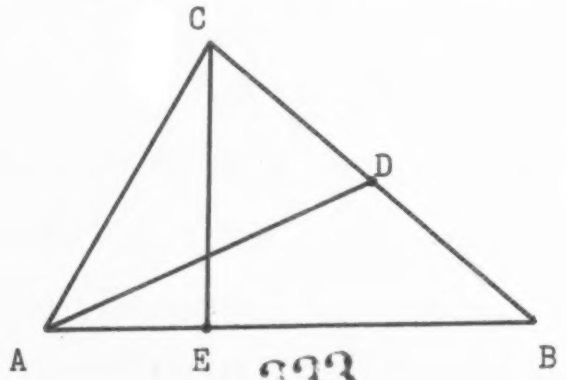
7. Using the data in Exercise 6 find the coordinates of the midpoint of

(a) $\overline{AB}$, and the slope of $\overleftrightarrow{AB}$.

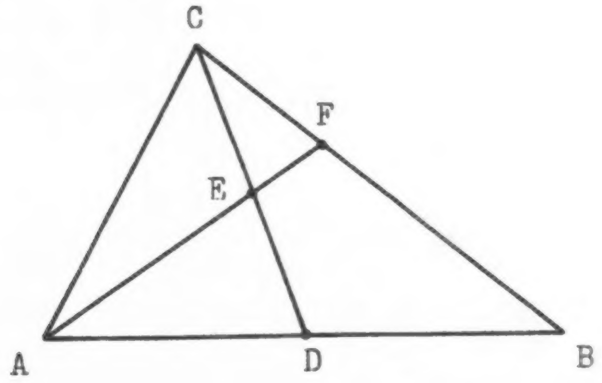
(b) $\overline{DE}$, and the slope of $\overleftrightarrow{DE}$.

(c) $\overline{KL}$, and the slope of $\overleftrightarrow{KL}$.

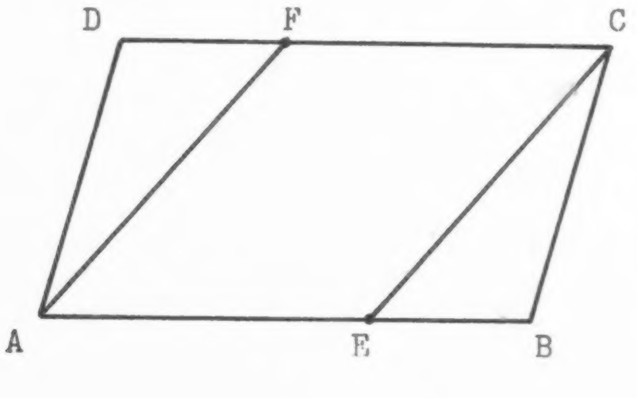
8. In $\triangle ABC$ let D be the midpoint of $\overline{BC}$ and E the trisection point of $\overline{AB}$ nearer A. Using equations for lines prove that $\overline{CE}$ bisects $\overline{AD}$.



9. Let $\overline{CD}$ be the median of ΔABC from C, and E is the midpoint of $\overline{CD}$. Let AE intersect $\overline{BC}$ in F. Find CF: FB.



10. In parallelogram ABCD, let E be the trisection point of $\overline{AB}$ nearer B, and F the trisection point of $\overline{CD}$ nearer D. Prove: $\overline{AC}$, $\overline{BD}$ and $\overline{FE}$ meet in a point.



11. Let $\angle C$ in ΔABC be a right angle. For the lengths given below for two sides of the triangle find the length of the third side.

(a) AC = 30, BC = 40	(b) AC = 2, BC = 3
(c) BC = 5, AB = 8	(d) AB = 12, BC = 5

12. Find the distance between the points in each pair listed below, if the coordinates given are for a certain rectangular coordinate system.

(a) A(3,2), B(9,2)	(b) C(-4,8), D(-4,-8)

(c) E(3,2), F(7,-1) (d) G(-2,8), H(3,-2)

13. A man walks 3 miles east, then 2 miles north, then 2 miles east. How far is he from his starting point. (Hint: Use a rectangular coordinate system and the distance formula.)

14. In a rectangular coordinate system the vertices of quadrilateral are A(0,0), B(2,4), C(8,6), D(6,2).

    (a) Prove that ABCD is a parallelogram.

    (b) If E is the midpoint of $\overline{AB}$, F is the midpoint of $\overline{BC}$, G is the midpoint of $\overline{CD}$ and H is the midpoint of $\overline{DA}$, show that EF = GH and FG = HE.

15. Prove that the line segment joining the midpoints of two sides of a triangle is half as long as the third side.

Index

Affine geometry, 126
Affine mapping, 273
Affine transformation on a line, 273
Antecedent, 17
Archimedean Property, 213, 253

Base, 268
Base points, 268
Between, 280
Biconditional Statement, 21

Collinear points, 132
Completeness Property, 245
Concurrent lines, 133
Conditional statement, 17
Connectives, 8
Consequent, 17
Coordinate systems on a line, 268
Coordinate systems on a plane, 293

Decimal, 250
Detachment, Rule of, 38
Diagonal of a quadrilateral, 310
Direct proof, 49
Distance between P and Q, (A, B-) 269
Distinct lines, points, 123
Division point: internal, 287

Equation for a line, 300
Equivalence class of parallel lines, 159
Equivalence relation, 158, 176
Equivalent statements, 22
Endpoint, 280
Existential quantifier, 29
Existential statement, 29

Factor, 221
Field, 194
Fraction, 206

Galois, Evariste, 62
Goldbach's Conjecture, 28
Group, 62, 67

Hypotenuse, 314

Incidence Axioms, 126
Incidence Relation, 126
Inclusive "or", 10
Indirect proof, 53
Inference from a universal statement, 40
Interior point, 280, 282
Intersection of two lines, 306
Irrational numbers, 246
Isomorphic, 113
Isomorphism, 90, 112

Lattice points, 149
Least upper bound, 237
Left operation property, 33
Length of a line segment, 238
Line, 120, 121, 149
Linear equation, 219

Median of triangle, 309
Midpoint, 284
Modus ponens, 38

Negation, 5
Non-commutative group, 76

Opposite rays, 282
Order of an element, 115
Order of a group, 115
Order relation (in a field), 208
Origin, 268

Parallel lines, 125
Parallelogram, 311
Parallelogram rule, 181
Parallel projection, 164, 166, 288
Permutations, 80
Plane, 120, 121, 149
Plane rectangular coordinate system, 319

Point, 120, 121, 149
Pythagorean property, 316

Quadratic equation, 221
Quadrilateral, 310
Quantified statements, 26

Ratio, 287
Ray, 282
Real number system, 244
Rectangle, 322
Right triangle, 314
Rule of detachment, 38

Segment, 280
Square root, 251
Statement, 3
Subgroup, 69
Substitution Principle for
   Equality, 32

Theorem, 128
Translation, 176
Triangle, 309
Truth table, 5

Unit-point, 268
Universal quantifiers, 27
Universal statement, 26
Upper bound, 236

Vector, 176
Vector polygon, 184

Zero vector, 187

END